

# $t$ -unique reductions for Mészáros's subdivision algebra

Darij Grinberg

version 1.0 (draft version), April 5, 2017

**Abstract.** Fix a commutative ring  $\mathbf{k}$ , an element  $\beta \in \mathbf{k}$  and a positive integer  $n$ . Let  $\mathcal{X}$  be the polynomial ring over  $\mathbf{k}$  in the  $n(n-1)/2$  indeterminates  $x_{i,j}$  for all  $1 \leq i < j \leq n$ . Consider the ideal  $\mathcal{J}_\beta$  of  $\mathcal{X}$  generated by all polynomials of the form  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta)$  for  $1 \leq i < j < k \leq n$ . The quotient algebra  $\mathcal{X}/\mathcal{J}_\beta$  (at least for a certain universal choice of  $\mathbf{k}$  and  $\beta$ ) has been introduced by Karola Mészáros in [Meszar09] as a commutative analogue of Anatol Kirillov's quasi-classical Yang-Baxter algebra. A natural question is to find a combinatorial basis of this quotient algebra. One can define the *pathless monomials*, i.e., the monomials in  $\mathcal{X}$  that have no divisors of the form  $x_{i,j}x_{j,k}$  with  $1 \leq i < j < k \leq n$ . The residue classes of these pathless monomials indeed span the  $\mathbf{k}$ -module  $\mathcal{X}/\mathcal{J}_\beta$ ; however, they turn out (in general) to be  $\mathbf{k}$ -linearly dependent. More combinatorially: Reducing a given monomial in  $\mathcal{X}$  modulo the ideal  $\mathcal{J}_\beta$  by applying replacements of the form  $x_{i,j}x_{j,k} \mapsto x_{i,k}(x_{i,j} + x_{j,k} + \beta)$  always eventually leads to a  $\mathbf{k}$ -linear combination of pathless monomials, but the result may depend on the choices made in the process.

More recently, the study of Grothendieck polynomials has led Laura Escobar and Karola Mészáros [EscMes15, §5] to defining a  $\mathbf{k}$ -algebra homomorphism  $D$  from  $\mathcal{X}$  into the polynomial ring  $\mathbf{k}[t_1, t_2, \dots, t_{n-1}]$  that sends each  $x_{i,j}$  to  $t_i$ . For a certain class of monomials  $m$  (those corresponding to “noncrossing trees”), they have shown that whatever result one gets by reducing  $m$  modulo  $\mathcal{J}_\beta$ , the image of this result under  $D$  is independent on the choices made in the reduction process. Mészáros has conjectured that this property holds not only for this class of monomials, but for any polynomial  $p \in \mathcal{X}$ . We prove this result, in the following slightly stronger form: If  $p \in \mathcal{X}$ , and if  $q \in \mathcal{X}$  is a  $\mathbf{k}$ -linear combination of pathless monomials satisfying  $p \equiv q \pmod{\mathcal{J}_\beta}$ , then  $D(q)$  does not depend on  $q$  (as long as  $\beta$  and  $p$  are fixed).

We also find an actual basis of the  $\mathbf{k}$ -module  $\mathcal{X}/\mathcal{J}_\beta$ , using what we call *forkless monomials*. We furthermore formulate a conjectural generalization.

## Contents

0.1. Acknowledgments . . . . .	5
<b>1. Definitions and results</b>	<b>6</b>
<b>2. The proof</b>	<b>8</b>
2.1. Preliminaries . . . . .	8
2.2. The algebra $\mathcal{Q}'$ of “zero-sum” power series . . . . .	8
2.3. The algebra homomorphism $A : \mathcal{X} \rightarrow \mathcal{Q}'$ . . . . .	9
2.4. The algebra $\mathcal{Q}$ of power series . . . . .	10
2.5. The continuous $\mathbf{k}$ -linear map $B : \mathcal{Q}' \rightarrow \mathcal{Q}$ . . . . .	10
2.6. The algebra $\mathcal{T}$ of power series . . . . .	14
2.7. The continuous $\mathbf{k}$ -algebra homomorphism $C : \mathcal{Q} \rightarrow \mathcal{T}$ . . . . .	14
2.8. Pathless monomials and subsets $S$ of $[n - 1]$ . . . . .	14
2.9. $D(q) = (C \circ B \circ A)(q)$ for pathless $q$ . . . . .	21
2.10. Proof of Theorem 1.7 for $\beta = 1$ . . . . .	21
2.11. Proof of Theorem 1.7 for $\beta$ regular . . . . .	22
2.12. Proof of Theorem 1.7 for all $\beta$ . . . . .	24
2.13. Appendix: Detailed proof of Proposition 1.5 . . . . .	29
<b>3. Forkless polynomials and a basis of <math>\mathcal{X}/\mathcal{J}_\beta</math></b>	<b>33</b>
3.1. Statements . . . . .	33
3.2. A reminder on Gröbner bases . . . . .	34
3.3. The proofs . . . . .	38
<b>4. A generalization?</b>	<b>39</b>

## Introduction

The main result of this paper is probably best illustrated by an example:

**Example 0.1.** Let us play a solitaire game. Fix a positive integer  $n$  and a number  $\beta \in \mathbb{Q}$ , and let  $\mathcal{X}$  be the ring  $\mathbb{Q}[x_{i,j} \mid 1 \leq i < j \leq n]$  of polynomials with rational coefficients in the  $n(n-1)/2$  indeterminates  $x_{i,j}$  with  $1 \leq i < j \leq n$ . (For example, if  $n = 4$ , then  $\mathcal{X} = \mathbb{Q}[x_{1,2}, x_{1,3}, x_{1,4}, x_{2,3}, x_{2,4}, x_{3,4}]$ .)

Start with any polynomial  $p \in \mathcal{X}$ . The allowed move is the following: Pick a monomial  $m$  that appears (with nonzero coefficient) in  $p$  and that is divisible by  $x_{i,j}x_{j,k}$  for some  $1 \leq i < j < k \leq n$ . For example,  $x_{1,2}x_{1,3}x_{2,4}$  is such a

monomial (if it appears in  $p$  and if  $n \geq 4$ ), because it is divisible by  $x_{i,j}x_{j,k}$  for  $(i, j, k) = (1, 2, 4)$ . Choose one triple  $(i, j, k)$  with  $1 \leq i < j < k \leq n$  and  $x_{i,j}x_{j,k} \mid m$  (sometimes, there are several choices). Now, replace this monomial  $m$  by  $\frac{x_{i,k}(x_{i,j} + x_{j,k} + \beta)}{x_{i,j}x_{j,k}}m$  in  $p$ .

Thus, each move modifies the polynomial, replacing a monomial by a sum of three monomials (or two, if  $\beta = 0$ ). The game ends when no more moves are possible (i.e., no monomial  $m$  appearing in your polynomial is divisible by  $x_{i,j}x_{j,k}$  for any  $1 \leq i < j < k \leq n$ ).

It is easy to see that this game (a thinly veiled reduction procedure modulo an ideal of  $\mathcal{X}$ ) always ends after finitely many moves. Here is one instance of this game being played, for  $n = 4$  and  $\beta = 1$  and starting with the polynomial  $p = x_{1,2}x_{2,3}x_{3,4}$ :

$$\begin{aligned}
& x_{1,2}x_{2,3}x_{3,4} \\
& \mapsto x_{1,3}(x_{1,2} + x_{2,3} + 1)x_{3,4} \\
& \quad (\text{here, we chose } m = x_{1,2}x_{2,3}x_{3,4} \text{ and } (i, j, k) = (1, 2, 3)) \\
& = x_{1,2}x_{1,3}x_{3,4} + x_{1,3}x_{2,3}x_{3,4} + x_{1,3}x_{3,4} \\
& \mapsto x_{1,2}x_{1,4}(x_{1,3} + x_{3,4} + 1) + x_{1,3}x_{2,3}x_{3,4} + x_{1,3}x_{3,4} \\
& \quad (\text{here, we chose } m = x_{1,2}x_{1,3}x_{3,4} \text{ and } (i, j, k) = (1, 3, 4)) \\
& = x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,2}x_{1,4} + x_{1,3}x_{2,3}x_{3,4} + x_{1,3}x_{3,4} \\
& \mapsto x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,2}x_{1,4} + x_{1,3}x_{2,4}(x_{2,3} + x_{3,4} + 1) + x_{1,3}x_{3,4} \\
& \quad (\text{here, we chose } m = x_{1,3}x_{2,3}x_{3,4} \text{ and } (i, j, k) = (2, 3, 4)) \\
& = x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,2}x_{1,4} + x_{1,3}x_{2,3}x_{2,4} + x_{1,3}x_{2,4}x_{3,4} + x_{1,3}x_{2,4} \\
& \quad + x_{1,3}x_{3,4} \\
& \mapsto x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,2}x_{1,4} + x_{1,3}x_{2,3}x_{2,4} + x_{1,3}x_{2,4}x_{3,4} + x_{1,3}x_{2,4} \\
& \quad + x_{1,4}(x_{1,3} + x_{3,4} + 1) \\
& \quad (\text{here, we chose } m = x_{1,3}x_{3,4} \text{ and } (i, j, k) = (1, 3, 4)) \\
& = x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,2}x_{1,4} + x_{1,3}x_{2,3}x_{2,4} + x_{1,3}x_{2,4}x_{3,4} \\
& \quad + x_{1,3}x_{2,4} + x_{1,3}x_{1,4} + x_{1,4}x_{3,4} + x_{1,4} \\
& \mapsto x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,2}x_{1,4} + x_{1,3}x_{2,3}x_{2,4} + x_{2,4}x_{1,4}(x_{1,3} + x_{3,4} + 1) \\
& \quad + x_{1,3}x_{2,4} + x_{1,3}x_{1,4} + x_{1,4}x_{3,4} + x_{1,4} \\
& \quad (\text{here, we chose } m = x_{1,3}x_{2,4}x_{3,4} \text{ and } (i, j, k) = (1, 3, 4)) \\
& = x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,2}x_{1,4} + x_{1,3}x_{2,3}x_{2,4} + x_{1,3}x_{1,4}x_{2,4} \\
& \quad + x_{1,4}x_{2,4}x_{3,4} + x_{1,4}x_{2,4} + x_{1,3}x_{2,4} + x_{1,3}x_{1,4} + x_{1,4}x_{3,4} + x_{1,4}. \tag{1}
\end{aligned}$$

The game ends at this polynomial, since there are no more moves to be done.

A standard question about games like this is: Is the state obtained at the end of the game (i.e., in our case, the polynomial after the game has ended) independent of the choices made during the game? In our case, the answer is

“no” (in general, for  $n \geq 4$ ). Indeed, the reader can easily verify that the above game could have led to a different result if we had made different choices.

However, something else turns out to be independent of the choices. Namely, let us transform the polynomial at the end of the game further by applying the substitution  $x_{i,j} \mapsto t_i$  (where  $t_1, t_2, \dots, t_{n-1}$  are new indeterminates). For example, doing this to the polynomial (1) results in

$$\begin{aligned} & t_1 t_1 t_1 + t_1 t_1 t_3 + t_1 t_1 + t_1 t_2 t_2 + t_1 t_1 t_2 + t_1 t_2 t_3 + t_1 t_2 + t_1 t_2 + t_1 t_1 + t_1 t_3 + t_1 \\ & = t_1 \left( 2t_1 + 2t_2 + t_3 + t_1^2 + t_2^2 + t_1 t_2 + t_1 t_3 + t_2 t_3 + 1 \right). \end{aligned}$$

According to a conjecture of Mészáros, the result of this substitution is indeed independent of the choices made during the game (as long as  $p$  is fixed).

Why would one play a game like this? The interest in the reduction rule  $m \mapsto \frac{x_{i,k}(x_{i,j} + x_{j,k} + \beta)}{x_{i,j}x_{j,k}}m$  originates in Karola Mészáros’s study [Meszar09] of the abelianization of Anatol Kirillov’s quasi-classical Yang-Baxter algebra (see, e.g., [Kirill16] for a recent survey of the latter and its many variants). To define this abelianization<sup>1</sup>, we let  $\beta$  be an indeterminate (unlike in Example 0.1, where it was an element of  $\mathbb{Q}$ ). Furthermore, fix a positive integer  $n$ . The abelianization of the  $(n$ -th) quasi-classical Yang-Baxter algebra is the commutative  $\mathbb{Q}[\beta]$ -algebra  $\mathcal{S}(A_n)$  with

$$\begin{array}{lll} \text{generators} & x_{i,j} & \text{for all } 1 \leq i < j \leq n \quad \text{and} \\ \text{relations} & x_{i,j}x_{j,k} = x_{i,k}(x_{i,j} + x_{j,k} + \beta) & \text{for all } 1 \leq i < j < k \leq n. \end{array}$$

A natural question is to find an explicit basis of  $\mathcal{S}(A_n)$  (as a  $\mathbb{Q}$ -vector space, or, if possible, as a  $\mathbb{Q}[\beta]$ -module). One might try constructing such a basis using a reduction algorithm (or “straightening law”) that takes any element of  $\mathcal{S}(A_n)$  (written as any polynomial in the generators  $x_{i,j}$ ) and rewrites it in a “normal form”. The most obvious way one could try to construct such a reduction algorithm is by repeatedly rewriting products of the form  $x_{i,j}x_{j,k}$  (with  $1 \leq i < j < k \leq n$ ) as  $x_{i,k}(x_{i,j} + x_{j,k} + \beta)$ , until this is no longer possible. This is precisely the game that we played in Example 0.1 (with the only difference that  $\beta$  is now an indeterminate, not a number). Unfortunately, the result of the game turns out to depend on the choices made while playing it; consequently, the “normal form” it constructs is not literally a normal form, and instead of a basis of  $\mathcal{S}(A_n)$  we only obtain a spanning set.<sup>2</sup>

<sup>1</sup>The notations used in this Introduction are meant to be provisional. In the rest of this paper, we shall work with different notations (and in a more general setting), which will be introduced in Section 1.

<sup>2</sup>Surprisingly, a similar reduction algorithm **does** work for the (non-abelianized) quasi-classical Yang-Baxter algebra itself. This is one of Mészáros’s results ([Meszar09, Theorem 30]).

Nevertheless, the result of the game is not meaningless. The idea to substitute  $t_i$  for  $x_{i,j}$  (in the result, not in the original polynomial!) seems to have appeared in work of Postnikov, Stanley and Mészáros; some concrete formulas (for specific values of the initial polynomial and specific values of  $\beta$ ) appear in [Stan15, Exercise A22]. Recent work on Grothendieck polynomials by Laura Escobar and Karola Mészáros [EscMes15, §5] has again brought up the notion of substituting  $t_i$  for  $x_{i,j}$  in the polynomial obtained at the end of the game. This has led Mészáros to the conjecture that, after this substitution, the resulting polynomial no longer depends on the choices made during the game. She has proven this conjecture for a certain class of polynomials (those corresponding to “noncrossing trees”).

The main purpose of this paper is to establish Mészáros’s conjecture in the general case. We shall, in fact, work in somewhat greater generality than all previously published sources. Instead of requiring  $\beta$  to be either a rational number (as in Example 0.1) or an indeterminate over  $\mathbb{Q}$  (as in the definition of  $\mathcal{S}(A_n)$ ), we shall let  $\beta$  be any element of the ground ring, which in turn will be an arbitrary commutative ring  $\mathbf{k}$ . Rather than working in an algebra like  $\mathcal{S}(A_n)$ , we shall work in the polynomial ring  $\mathcal{X} = \mathbf{k}[x_{i,j} \mid 1 \leq i < j \leq n]$ , and study the ideal  $\mathcal{J}_\beta$  generated by all elements of the form  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta)$  for  $1 \leq i < j < k \leq n$ . Instead of focussing on the reduction algorithm, we shall generally study polynomials in  $\mathcal{X}$  that are congruent to each other modulo the ideal  $\mathcal{J}_\beta$ . A monomial in  $\mathcal{X}$  will be called “pathless” if it is not divisible by any monomial of the form  $x_{i,j}x_{j,k}$  with  $i < j < k$ . A polynomial in  $\mathcal{X}$  will be called “pathless” if all monomials appearing in it are pathless. Thus, “pathless” polynomials are precisely the polynomials  $p \in \mathcal{X}$  for which the game in Example 0.1 would end immediately if started at  $p$ . Our main result (Theorem 1.7) will show that if  $p \in \mathcal{X}$  is a polynomial, and if  $q \in \mathcal{X}$  is a pathless polynomial congruent to  $p$  modulo  $\mathcal{J}_\beta$ , then the image of  $q$  under the substitution  $x_{i,j} \mapsto t_i$  does not depend on  $q$  (but only on  $\beta$  and  $p$ ). This, in particular, yields Mészáros’s conjecture; but it is a stronger result, because it does not require that  $q$  is obtained from  $p$  by playing the game from Example 0.1 (all we ask for is that  $q$  be pathless and congruent to  $p$  modulo  $\mathcal{J}_\beta$ ).

After the proof of Theorem 1.7, we shall also outline an answer (Proposition 3.4) to the (easier) question of finding a basis for the quotient ring  $\mathcal{X}/\mathcal{J}_\beta$ . This basis will be obtained using an explicitly given Gröbner basis of the ideal  $\mathcal{J}_\beta$ . Finally, we shall conjecture a generalization (Conjecture 4.3) of Theorem 1.7 to an ideal  $\mathcal{J}_{\beta,\alpha}$  that “deforms”  $\mathcal{J}_\beta$ .

## 0.1. Acknowledgments

The SageMath computer algebra system [SageMath] was of great service during the development of the results below.

# 1. Definitions and results

Let us now start from scratch, and set the stage for the main result.

**Definition 1.1.** Let  $\mathbb{N} = \{0, 1, 2, \dots\}$ .

Let  $[m]$  be the set  $\{1, 2, \dots, m\}$  for each  $m \in \mathbb{N}$ .

Let  $\mathbf{k}$  be a commutative ring. (We fix  $\mathbf{k}$  throughout this paper.)

The word “monomial” shall always mean an element of a free abelian monoid (written multiplicatively). For example, the monomials in two indeterminates  $x$  and  $y$  are the elements of the form  $x^i y^j$  with  $(i, j) \in \mathbb{N}^2$ . Thus, monomials do not include coefficients (and are not bound to a specific base ring).

**Definition 1.2.** Fix a positive integer  $n$ . Let  $\mathcal{X}$  be the polynomial ring

$$\mathbf{k} \left[ x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j \right].$$

This is a polynomial ring in  $n(n-1)/2$  indeterminates  $x_{i,j}$  over  $\mathbf{k}$ .

We shall use the notation  $\mathfrak{M}$  for the set of all monomials in these indeterminates  $x_{i,j}$ . Notice that  $\mathfrak{M}$  is an abelian monoid under multiplication.

**Definition 1.3.** A monomial  $\mathfrak{m} \in \mathfrak{M}$  is said to be *pathless* if there exists no triple  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$  and  $x_{i,j} x_{j,k} \mid \mathfrak{m}$  (as monomials).

A polynomial  $p \in \mathcal{X}$  is said to be *pathless* if it is a  $\mathbf{k}$ -linear combination of pathless monomials.

**Definition 1.4.** Let  $\beta \in \mathbf{k}$ . Let  $\mathcal{J}_\beta$  be the ideal of  $\mathcal{X}$  generated by all elements of the form  $x_{i,j} x_{j,k} - x_{i,k} (x_{i,j} + x_{j,k} + \beta)$  for  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$ .

The following fact is easy to check:

**Proposition 1.5.** Let  $\beta \in \mathbf{k}$  and  $p \in \mathcal{X}$ . Then, there exists a pathless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_\beta}$ .

In general, this  $q$  is not unique.<sup>3</sup>

---

<sup>3</sup>For instance, if  $\mathbf{k} = \mathbb{Z}$ ,  $\beta = 1$  and  $n = 4$ , then

$$\begin{aligned} q_1 = & x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,3}x_{1,4} + x_{1,3}x_{1,4}x_{2,4} + x_{1,3}x_{2,3}x_{2,4} \\ & + x_{1,3}x_{2,4} + x_{1,4} + x_{1,4}x_{2,4} + x_{1,4}x_{2,4}x_{3,4} + x_{1,4}x_{3,4} \end{aligned}$$

and

$$\begin{aligned} q_2 = & x_{1,2}x_{1,3}x_{1,4} + x_{1,2}x_{1,4} + x_{1,2}x_{1,4}x_{3,4} + x_{1,3}x_{1,4} + x_{1,3}x_{1,4}x_{2,3} \\ & + x_{1,4} + x_{1,4}x_{2,3} + x_{1,4}x_{2,3}x_{2,4} + x_{1,4}x_{2,4} + x_{1,4}x_{2,4}x_{3,4} + x_{1,4}x_{3,4} \end{aligned}$$

are two pathless polynomials  $q \in \mathcal{X}$  satisfying  $x_{1,2}x_{2,3}x_{3,4} \equiv q \pmod{\mathcal{J}_\beta}$ , but they are not identical.

We shall roughly outline a proof of Proposition 1.5 now; a more detailed writeup of this proof can be found in Section 2.13 below.

*Proof of Proposition 1.5 (sketched).* The *weight* of a monomial  $\prod_{\substack{(i,j) \in [n]^2; \\ i < j}} x_{i,j}^{a_{i,j}} \in \mathfrak{M}$  shall

mean the nonnegative integer  $\sum_{\substack{(i,j) \in [n]^2; \\ i < j}} a_{i,j} (n - j + i)$ . If we have a monomial

$\mathfrak{m} \in \mathfrak{M}$  that is not pathless, then we can find a triple  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$  and  $x_{i,j}x_{j,k} \mid \mathfrak{m}$ ; then, we can replace  $\mathfrak{m}$  by a polynomial

$\tilde{\mathfrak{m}} = \mathfrak{m} \cdot \frac{x_{i,k} (x_{i,j} + x_{j,k} + \beta)}{x_{i,j}x_{j,k}}$ , which is congruent to  $\mathfrak{m}$  modulo  $\mathcal{J}_\beta$  but has the

property that all monomials appearing in it have a smaller weight than  $\mathfrak{m}$ . This gives rise to a recursive algorithm for reducing a polynomial modulo the ideal  $\mathcal{J}_\beta$ . The procedure will necessarily terminate (although its result might depend on the order of operation); the polynomial resulting at its end will be pathless.  $\square$

The ideal  $\mathcal{J}_\beta$  is relevant to the so-called *subdivision algebra of root polytopes* (denoted by  $\mathcal{S}(\beta)$  in [EscMes15, §5] and  $\mathcal{S}(A_n)$  in [Meszar09, §1]). Namely, this latter algebra is defined as the quotient  $\mathcal{X}/\mathcal{J}_\beta$  for a certain choice of  $\mathbf{k}$  and  $\beta$  (namely, for the choice where  $\mathbf{k}$  is a univariate polynomial ring over  $\mathbb{Q}$ , and  $\beta$  is the indeterminate in  $\mathbf{k}$ ). This algebra was first introduced by Mészáros in [Meszar09] as the abelianization of Anatol Kirillov’s quasi-classical Yang-Baxter algebra.

In [EscMes15, §5 and §7], Escobar and Mészáros (motivated by computations of Grothendieck polynomials) consider the result of substituting  $t_i$  for each variable  $x_{i,j}$  in a polynomial  $f \in \mathcal{X}$ . In our language, this leads to the following definition:

**Definition 1.6.** Let  $\mathcal{T}'$  be the polynomial ring  $\mathbf{k}[t_1, t_2, \dots, t_{n-1}]$ . We define a  $\mathbf{k}$ -algebra homomorphism  $D : \mathcal{X} \rightarrow \mathcal{T}'$  by

$$D(x_{i,j}) = t_i \quad \text{for every } (i, j) \in [n]^2 \text{ satisfying } i < j.$$

The goal of this paper is to prove the following fact, which was conjectured by Karola Mészáros in a 2015 talk at MIT:

**Theorem 1.7.** Let  $\beta \in \mathbf{k}$  and  $p \in \mathcal{X}$ . Consider any pathless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_\beta}$ . Then,  $D(q)$  does not depend on the choice of  $q$  (but merely on the choice of  $\beta$  and  $p$ ).

It is not generally true that  $D(q) = D(p)$ ; thus, Theorem 1.7 does not follow from a simple “invariant”.

## 2. The proof

### 2.1. Preliminaries

The proof of Theorem 1.7 will occupy most of this paper. It proceeds in several steps. First, we shall define three  $\mathbf{k}$ -algebras  $\mathcal{Q}'$ ,  $\mathcal{Q}$  and  $\mathcal{T}$  and three  $\mathbf{k}$ -linear maps  $A$ ,  $B$  and  $C$  (with  $A$  and  $C$  being  $\mathbf{k}$ -algebra homomorphism) forming a diagram

$$\mathcal{X} \xrightarrow{A} \mathcal{Q}' \xrightarrow{B} \mathcal{Q} \xrightarrow{C} \mathcal{T}.$$

We shall eventually show that:

- (Proposition 2.5 below) the homomorphism  $A$  annihilates the ideal  $\mathcal{I}_1$ , but
- (Corollary 2.19 below) each pathless polynomial  $q$  satisfies  $D(q) = (C \circ B \circ A)(q)$  (the equation makes sense since  $\mathcal{T}' \subseteq \mathcal{T}$ ).

These two facts will allow us to prove Theorem 1.7 in the case when  $\beta = 1$  (this is Lemma 2.21 below). From this case, we shall then escalate to a somewhat more general case: Namely, we shall prove Theorem 1.7 in the case when  $\beta$  is regular<sup>4</sup> (Proposition 2.24). This latter case already covers the situation studied in [EscMes15, §5] (indeed,  $\beta$  is a polynomial indeterminate over  $\mathbf{k} = \mathbb{Q}$  in this case). Finally, using this case as a stepping stone, we shall obtain a proof of Theorem 1.7 in full generality.

Let us define the notion of a regular element of a commutative ring:

**Definition 2.1.** Let  $\mathbf{k}$  be a commutative ring. Let  $a \in \mathbf{k}$ . The element  $a$  of  $\mathbf{k}$  is said to be *regular* if and only if every  $x \in \mathbf{k}$  satisfying  $ax = 0$  satisfies  $x = 0$ .

### 2.2. The algebra $\mathcal{Q}'$ of “zero-sum” power series

**Definition 2.2. (a)** Set  $\mathcal{Q}' = \mathbf{k}[[r_1, r_2, \dots, r_{n-1}]]$ . (This is the ring of power series in the  $n - 1$  indeterminates  $r_1, r_2, \dots, r_{n-1}$  over  $\mathbf{k}$ .)

The  $\mathbf{k}$ -algebra  $\mathcal{Q}'$  has a topology: the product topology, defined by regarding it as a direct product of many copies of  $\mathbf{k}$  (thus regarding each power series as the family of its coefficients). (Each copy of  $\mathbf{k}$  corresponds to a monomial.) Thus,  $\mathcal{Q}'$  becomes a topological  $\mathbf{k}$ -algebra. Every ring of power series in this note will be endowed with a topology in this very way.

**(b)** For each  $i \in [n]$ , we define a monomial  $q_i$  in the indeterminates  $r_1, r_2, \dots, r_{n-1}$  by  $q_i = r_i r_{i+1} \cdots r_{n-1}$ . (In particular,  $q_n = 1$ .)

Each of the elements  $q_1, q_2, \dots, q_n$  of  $\mathcal{Q}'$  is regular (since it is a monomial), and they satisfy  $q_n \mid q_{n-1} \mid \cdots \mid q_1$ . Hence, it makes sense to speak of quotients such as  $q_i/q_j$  for  $1 \leq i \leq j \leq n$ . Explicitly,  $q_i/q_j = r_i r_{i+1} \cdots r_{j-1}$  whenever  $1 \leq i \leq j \leq n$ .

<sup>4</sup>See Definition 2.1 for the meaning of “regular”.



It is easy to see that

$$q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n} = r_1^{a_1} r_2^{a_1+a_2} r_3^{a_1+a_2+a_3} \cdots r_{n-1}^{a_1+a_2+\cdots+a_{n-1}} \quad (2)$$

for all  $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$ . Also,

$$r_1^{b_1} r_2^{b_2} \cdots r_{n-1}^{b_{n-1}} = q_1^{b_1} q_2^{b_2-b_1} q_3^{b_3-b_2} \cdots q_{n-1}^{b_{n-1}-b_{n-2}} q_n^{-b_{n-1}} \quad (3)$$

for all  $(b_1, b_2, \dots, b_{n-1}) \in \mathbb{Z}^{n-1}$ .

**Definition 2.3.** Let  $\mathfrak{Z}$  denote the set of all  $n$ -tuples  $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$  satisfying  $a_1 + a_2 + \cdots + a_n = 0$  and  $a_1 + a_2 + \cdots + a_i \geq 0$  for all  $i \in \{1, 2, \dots, n\}$ .

The topological  $\mathbf{k}$ -module  $\mathcal{Q}'$  has a topological basis<sup>5</sup>  $(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n})_{(a_1, a_2, \dots, a_n) \in \mathfrak{Z}}$ . Indeed, this is just a reindexing of the standard topological basis  $(r_1^{b_1} r_2^{b_2} \cdots r_{n-1}^{b_{n-1}})_{(b_1, b_2, \dots, b_{n-1}) \in \mathbb{N}^{n-1}}$  via the bijection

$$\begin{aligned} \mathfrak{Z} &\rightarrow \mathbb{N}^{n-1}, \\ (a_1, a_2, \dots, a_n) &\mapsto (a_1, a_1 + a_2, a_1 + a_2 + a_3, \dots, a_1 + a_2 + \cdots + a_{n-1}) \end{aligned}$$

(because of the equality (2)).

### 2.3. The algebra homomorphism $A : \mathcal{X} \rightarrow \mathcal{Q}'$

**Definition 2.4.** Define a  $\mathbf{k}$ -algebra homomorphism  $A : \mathcal{X} \rightarrow \mathcal{Q}'$  by

$$A(x_{i,j}) = \frac{q_i/q_j}{1 - q_i/q_j} = \sum_{k \geq 0} (q_i/q_j)^k \quad \text{for all } (i, j) \in [n]^2 \text{ satisfying } i < j.$$

Notice that this is well-defined, since  $q_i/q_j = r_i r_{i+1} \cdots r_{j-1} \in \mathcal{Q}'$  is homogeneous of positive degree and thus can be substituted into a power series.

<sup>5</sup>The notion of a “topological basis” that we are using here has nothing to do with the concept of a basis of a topology (also known as “base”). Instead, it is merely an analogue of the concept of a basis of a  $\mathbf{k}$ -module. It is defined as follows:

A *topological basis* of a topological  $\mathbf{k}$ -module  $\mathcal{M}$  means a family  $(m_s)_{s \in \mathfrak{S}} \in \mathcal{M}^{\mathfrak{S}}$  with the following two properties:

- For each family  $(\lambda_s)_{s \in \mathfrak{S}} \in \mathbf{k}^{\mathfrak{S}}$ , the sum  $\sum_{s \in \mathfrak{S}} \lambda_s m_s$  converges with respect to the topology on  $\mathcal{M}$ . (Such a sum is called an *infinite  $\mathbf{k}$ -linear combination* of the family  $(m_s)_{s \in \mathfrak{S}}$ .)
- Each element of  $\mathcal{M}$  can be uniquely represented in the form  $\sum_{s \in \mathfrak{S}} \lambda_s m_s$  for some family  $(\lambda_s)_{s \in \mathfrak{S}} \in \mathbf{k}^{\mathfrak{S}}$ .

For example,  $(r_1^{b_1} r_2^{b_2} \cdots r_{n-1}^{b_{n-1}})_{(b_1, b_2, \dots, b_{n-1}) \in \mathbb{N}^{n-1}}$  is a topological basis of the topological  $\mathbf{k}$ -module  $\mathcal{Q}'$ , because each power series can be uniquely represented as an infinite  $\mathbf{k}$ -linear combination of all the monomials.

**Proposition 2.5.** We have  $A(\mathcal{J}_1) = 0$ .

*Proof of Proposition 2.5.* The ideal  $\mathcal{J}_1$  of  $\mathcal{X}$  is generated by all elements of the form  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + 1)$  for  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$ . Thus, it suffices to show that  $A(x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + 1)) = 0$  for all triples  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$ . So let us fix such a triple.

Set  $y = q_i/q_j$  and  $z = q_j/q_k$ . Both  $y$  and  $z$  are homogeneous of positive degree, and thus we can freely divide by power series such as  $1 - y$  and  $1 - z$ .

The definition of  $A$  yields  $A(x_{i,j}) = \frac{q_i/q_j}{1 - q_i/q_j} = \frac{y}{1 - y}$  (since  $q_i/q_j = y$ ).

Similarly,  $A(x_{j,k}) = \frac{z}{1 - z}$ .

The definition of  $A$  yields  $A(x_{i,k}) = \frac{q_i/q_k}{1 - q_i/q_k} = \frac{yz}{1 - yz}$  (since  $q_i/q_k = \underbrace{(q_i/q_j)}_{=y} \underbrace{(q_j/q_k)}_{=z} = yz$ ).

But  $A$  is a  $\mathbf{k}$ -algebra homomorphism. Thus,

$$\begin{aligned} & A(x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + 1)) \\ &= \underbrace{A(x_{i,j})}_{= \frac{y}{1-y}} \underbrace{A(x_{j,k})}_{= \frac{z}{1-z}} - \underbrace{A(x_{i,k})}_{= \frac{yz}{1-yz}} \left( \underbrace{A(x_{i,j})}_{= \frac{y}{1-y}} + \underbrace{A(x_{j,k})}_{= \frac{z}{1-z}} + 1 \right) \\ &= \frac{y}{1-y} \frac{z}{1-z} - \frac{yz}{1-yz} \left( \frac{y}{1-y} + \frac{z}{1-z} + 1 \right) \\ &= 0, \end{aligned}$$

qed. □

## 2.4. The algebra $\mathcal{Q}$ of power series

**Definition 2.6.** Let  $\mathcal{Q}$  be the  $\mathbf{k}$ -algebra  $\mathbf{k}[[q_1, q_2, \dots, q_{n-1}]]$ . This is the ring of formal power series in the  $n - 1$  indeterminates  $q_1, q_2, \dots, q_{n-1}$  over  $\mathbf{k}$ . These indeterminates have nothing to do with the monomials  $q_i$  from Definition 2.2 (a) (but of course the same names have been chosen for similarity).

The topology on  $\mathcal{Q}$  shall be the usual one (i.e., the one defined similarly to the one on  $\mathcal{Q}'$ ).

## 2.5. The continuous $\mathbf{k}$ -linear map $B : \mathcal{Q}' \rightarrow \mathcal{Q}$

Before we define our next map, let us show three simple lemmas:

**Lemma 2.7.** Let  $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$  be such that  $a_1 + a_2 + \dots + a_n = 0$ . Let  $N = \sum_{i \in [n]} \max \{a_i, 0\}$ . Then,  $(a_1, a_2, \dots, a_n) \in \{-N, -N+1, \dots, N\}^n$ .

*Proof of Lemma 2.7.* We have

$$0 = a_1 + a_2 + \dots + a_n = \sum_{i \in [n]} a_i = \sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i + \sum_{\substack{i \in [n]; \\ a_i < 0}} a_i$$

(since each  $i \in [n]$  satisfies either  $a_i \geq 0$  or  $a_i < 0$ , but not both). Solving this equation for  $\sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i$ , we obtain

$$\sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i = - \sum_{\substack{i \in [n]; \\ a_i < 0}} a_i = \sum_{\substack{i \in [n]; \\ a_i < 0}} \underbrace{(-a_i)}_{=|a_i| \text{ (since } a_i < 0)} = \sum_{\substack{i \in [n]; \\ a_i < 0}} |a_i|.$$

But

$$\begin{aligned} N &= \sum_{i \in [n]} \max \{a_i, 0\} = \sum_{\substack{i \in [n]; \\ a_i \geq 0}} \underbrace{\max \{a_i, 0\}}_{=a_i \text{ (since } a_i \geq 0)}} + \sum_{\substack{i \in [n]; \\ a_i < 0}} \underbrace{\max \{a_i, 0\}}_{=0 \text{ (since } a_i < 0)}} \\ &\quad \text{(since each } i \in [n] \text{ satisfies either } a_i \geq 0 \text{ or } a_i < 0, \text{ but not both)} \\ &= \sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i + \underbrace{\sum_{\substack{i \in [n]; \\ a_i < 0}} 0}_{=0} = \sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i = \sum_{\substack{i \in [n]; \\ a_i < 0}} |a_i|. \end{aligned}$$

Now, we claim that

$$|a_j| \leq N \quad \text{for each } j \in [n]. \quad (4)$$

[Proof of (4): Fix  $j \in [n]$ . We want to prove (4). We are in one of the following two cases:

Case 1: We have  $a_j \geq 0$ .

Case 2: We have  $a_j < 0$ .

Let us consider Case 1 first. In this case, we have  $a_j \geq 0$ . Thus,  $a_j$  is an addend in the sum  $\sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i$ . Since this sum consists purely of nonnegative integers<sup>6</sup>, we

therefore conclude that  $a_j$  is at most as large as this sum. In other words,  $a_j \leq \sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i$ . In light of  $N = \sum_{\substack{i \in [n]; \\ a_i \geq 0}} a_i$ , this rewrites as  $a_j \leq N$ . But  $a_j \geq 0$  and thus  $|a_j| = a_j \leq N$ . Hence, (4) is proven in Case 1.

<sup>6</sup>because  $a_i$  is a nonnegative integer for each  $i \in [n]$  satisfying  $a_i \geq 0$

Let us now consider Case 2. In this case, we have  $a_j < 0$ . Hence,  $|a_j|$  is an addend in the sum  $\sum_{\substack{i \in [n]; \\ a_i < 0}} |a_i|$ . Since this sum consists purely of nonnegative

integers<sup>7</sup>, we therefore conclude that its addend  $|a_j|$  is at most as large as the whole sum. In other words,  $|a_j| \leq \sum_{\substack{i \in [n]; \\ a_i < 0}} |a_i|$ . In light of  $N = \sum_{\substack{i \in [n]; \\ a_i < 0}} |a_i|$ , this rewrites

as  $|a_j| \leq N$ . Hence, (4) is proven in Case 2.

We have thus proven (4) in both Cases 1 and 2. Hence, (4) is proven.]

From (4), we conclude that  $a_j \in \{-N, -N+1, \dots, N\}$  for each  $j \in [n]$  (since  $a_j \in \mathbb{Z}$ ). Hence,  $(a_1, a_2, \dots, a_n) \in \{-N, -N+1, \dots, N\}^n$ . This proves Lemma 2.7.  $\square$

**Lemma 2.8.** Let  $b_1, b_2, \dots, b_{n-1}$  be  $n-1$  nonnegative integers. Let  $N = b_1 + b_2 + \dots + b_{n-1}$ . Let  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  be such that each  $i \in [n-1]$  satisfies  $b_i = \max\{a_i, 0\}$ . Then,  $(a_1, a_2, \dots, a_n)$  belongs to  $\{-N, -N+1, \dots, N\}^n$ .

*Proof of Lemma 2.8.* From  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$ , we obtain  $a_1 + a_2 + \dots + a_n = 0$  and  $a_1 + a_2 + \dots + a_i \geq 0$  for all  $i \in \{1, 2, \dots, n\}$ . From  $a_1 + a_2 + \dots + a_i \geq 0$  for all  $i \in \{1, 2, \dots, n\}$ , we obtain  $a_1 + a_2 + \dots + a_{n-1} \geq 0$ .<sup>8</sup>

Now,

$$0 = a_1 + a_2 + \dots + a_n = \underbrace{(a_1 + a_2 + \dots + a_{n-1})}_{\geq 0} + a_n \geq 0 + a_n = a_n,$$

so that  $a_n \leq 0$  and therefore  $\max\{a_n, 0\} = 0$ .

We know that each  $i \in [n-1]$  satisfies  $b_i = \max\{a_i, 0\}$ . Hence,  $\sum_{i \in [n-1]} b_i = \sum_{i \in [n-1]} \max\{a_i, 0\}$ . Thus,

$$\sum_{i \in [n-1]} \max\{a_i, 0\} = \sum_{i \in [n-1]} b_i = b_1 + b_2 + \dots + b_{n-1} = N.$$

Now,

$$\sum_{i \in [n]} \max\{a_i, 0\} = \underbrace{\sum_{i \in [n-1]} \max\{a_i, 0\}}_{=N} + \underbrace{\max\{a_n, 0\}}_{=0} = N + 0 = N.$$

In other words,  $N = \sum_{i \in [n]} \max\{a_i, 0\}$ . Hence, Lemma 2.7 shows that  $(a_1, a_2, \dots, a_n) \in \{-N, -N+1, \dots, N\}^n$ . This proves Lemma 2.8.  $\square$

<sup>7</sup>because  $|a_i|$  is a nonnegative integer for each  $i \in [n]$  satisfying  $a_i < 0$

<sup>8</sup>To be fully precise: The inequality  $a_1 + a_2 + \dots + a_{n-1} \geq 0$  follows from  $a_1 + a_2 + \dots + a_i \geq 0$  (applied to  $i = n-1$ ) when  $n \geq 2$ . But when  $n < 2$ , it follows from  $a_1 + a_2 + \dots + a_{n-1} =$  (empty sum)  $= 0$ .

**Lemma 2.9.** Let  $\mathbf{m}$  be a monomial in the indeterminates  $q_1, q_2, \dots, q_{n-1}$  (with nonnegative exponents). Then, there exist only finitely many  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  satisfying  $\prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} = \mathbf{m}$ . (Here, again,  $q_1, q_2, \dots, q_{n-1}$  are the indeterminates of  $\mathcal{Q}$ , not the monomials  $q_i$  from Definition 2.2 (b).)

*Proof of Lemma 2.9.* Write  $\mathbf{m}$  in the form  $\mathbf{m} = \prod_{i \in [n-1]} q_i^{b_i}$ . Let  $N = b_1 + b_2 + \dots + b_{n-1}$ . We want to prove that there exist only finitely many  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  satisfying  $\prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} = \mathbf{m}$ . We shall show that each such  $(a_1, a_2, \dots, a_n)$  must belong to the set  $\{-N, -N+1, \dots, N\}^n$ .

Indeed, let  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  be such that  $\prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} = \mathbf{m}$ . We must show that  $(a_1, a_2, \dots, a_n)$  belongs to  $\{-N, -N+1, \dots, N\}^n$ .

We have

$$\begin{aligned} \prod_{i \in [n-1]} q_i^{\max\{a_i, 0\}} &= \left( \prod_{\substack{i \in [n-1]; \\ a_i > 0}} \underbrace{q_i^{\max\{a_i, 0\}}}_{\substack{= q_i^{a_i} \\ (\text{since } \max\{a_i, 0\} = a_i \\ (\text{since } a_i > 0))}} \right) \left( \prod_{\substack{i \in [n-1]; \\ a_i \leq 0}} \underbrace{q_i^{\max\{a_i, 0\}}}_{\substack{= q_i^0 \\ (\text{since } \max\{a_i, 0\} = 0 \\ (\text{since } a_i \leq 0))}} \right) \\ &= \left( \prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} \right) \left( \prod_{\substack{i \in [n-1]; \\ a_i \leq 0}} \underbrace{q_i^0}_{=1} \right) = \prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} = \mathbf{m} = \prod_{i \in [n-1]} q_i^{b_i}. \end{aligned}$$

Thus,  $\prod_{i \in [n-1]} q_i^{b_i} = \prod_{i \in [n-1]} q_i^{\max\{a_i, 0\}}$ . In other words, each  $i \in [n-1]$  satisfies  $b_i = \max\{a_i, 0\}$ . Hence,  $(a_1, a_2, \dots, a_n)$  belongs to  $\{-N, -N+1, \dots, N\}^n$  (by Lemma 2.8).

Now, forget that we fixed  $(a_1, a_2, \dots, a_n)$ . We thus have shown that each  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  satisfying  $\prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} = \mathbf{m}$  must belong to the set  $\{-N, -N+1, \dots, N\}^n$ .

Therefore, there exist only finitely many such  $(a_1, a_2, \dots, a_n)$  (because the set  $\{-N, -N+1, \dots, N\}^n$  is finite). This proves Lemma 2.9.  $\square$

**Definition 2.10.** We define a continuous  $\mathbf{k}$ -linear map  $B : \mathcal{Q}' \rightarrow \mathcal{Q}$  by setting

$$B(q_1^{a_1} q_2^{a_2} \dots q_n^{a_n}) = \prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} \quad \text{for each } (a_1, a_2, \dots, a_n) \in \mathfrak{Z}.$$

This is well-defined, since  $(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n})_{(a_1, a_2, \dots, a_n) \in \mathfrak{Z}}$  is a topological basis of  $\mathcal{Q}'$ , and because of Lemma 2.9 (which guarantees convergence when the map  $B$  is applied to an infinite  $\mathbf{k}$ -linear combination of monomials).

Of course,  $B$  is (in general) not a  $\mathbf{k}$ -algebra homomorphism.

## 2.6. The algebra $\mathcal{T}$ of power series

**Definition 2.11.** We define a topological  $\mathbf{k}$ -algebra  $\mathcal{T}$  by  $\mathcal{T} = \mathbf{k}[[t_1, t_2, \dots, t_{n-1}]]$  (with the usual topology). Again, this is simply a ring of formal power series over  $\mathbf{k}$ .

We shall regard  $\mathcal{T}'$  as a  $\mathbf{k}$ -subalgebra of  $\mathcal{T}$  (in the obvious way). Thus,  $D : \mathcal{X} \rightarrow \mathcal{T}'$  becomes a  $\mathbf{k}$ -algebra homomorphism  $\mathcal{X} \rightarrow \mathcal{T}$ .

## 2.7. The continuous $\mathbf{k}$ -algebra homomorphism $C : \mathcal{Q} \rightarrow \mathcal{T}$

**Definition 2.12.** We define a continuous  $\mathbf{k}$ -algebra homomorphism  $C : \mathcal{Q} \rightarrow \mathcal{T}$  by

$$C(q_i) = \frac{t_i}{1 + t_i} \quad \text{for each } i \in [n-1].$$

This is well-defined, because for each  $i \in [n-1]$ , the power series  $\frac{t_i}{1 + t_i}$  has constant term 0 and thus can be substituted into power series.

Thus, we have defined the following spaces and maps between them:

$$\mathcal{X} \xrightarrow{A} \mathcal{Q}' \xrightarrow{B} \mathcal{Q} \xrightarrow{C} \mathcal{T}.$$

It is worth reminding ourselves that  $A$  and  $C$  are  $\mathbf{k}$ -algebra homomorphisms, but  $B$  (in general) is not.

## 2.8. Pathless monomials and subsets $S$ of $[n-1]$

Next, we want to study the action of the composition  $C \circ B \circ A$  on pathless monomials. We first introduce some more notations:

**Definition 2.13.** Let  $S$  be a subset of  $[n-1]$ .

(a) Let  $\mathfrak{P}_S$  be the set of all pairs  $(i, j) \in S \times ([n] \setminus S)$  satisfying  $i < j$ .

(b) A monomial  $\mathfrak{m} \in \mathfrak{M}$  is said to be *S-friendly* if it is a product of some of the indeterminates  $x_{i,j}$  with  $(i, j) \in \mathfrak{P}_S$ . In other words, a monomial  $\mathfrak{m} \in \mathfrak{M}$  is *S-friendly* if and only if every indeterminate  $x_{i,j}$  that appears in  $\mathfrak{m}$  satisfies  $i \in S$  and  $j \notin S$ .

We let  $\mathfrak{M}_S$  denote the set of all *S-friendly* monomials.

(c) We let  $\mathcal{X}_S$  denote the polynomial ring  $\mathbf{k}[x_{i,j} \mid (i,j) \in \mathfrak{P}_S]$ . This is clearly a subring of  $\mathcal{X}$ . The  $\mathbf{k}$ -module  $\mathcal{X}_S$  has a basis consisting of all  $S$ -friendly monomials  $\mathbf{m} \in \mathfrak{M}$ .

(d) An  $n$ -tuple  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  is said to be  $S$ -adequate if and only if it satisfies  $(a_i \geq 0 \text{ for all } i \in S)$  and  $(a_i \leq 0 \text{ for all } i \in [n] \setminus S)$ . Let  $\mathfrak{Z}_S$  denote the set of all  $S$ -adequate  $n$ -tuples  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$ . We let  $\mathcal{Q}'_S$  denote the subset of  $\mathcal{Q}'$  consisting of all infinite  $\mathbf{k}$ -linear combinations of the monomials  $q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$  for  $S$ -adequate  $n$ -tuples  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}_S$ . It is easy to see that  $\mathcal{Q}'_S$  is a topological  $\mathbf{k}$ -subalgebra of  $\mathcal{Q}'$  (since the entrywise sum of two  $S$ -adequate  $n$ -tuples is  $S$ -adequate again).

(At this point, it is helpful to recall once again that the  $q_1, q_2, \dots, q_n$  are not indeterminates here, but rather monomials defined by  $q_i = r_i r_{i+1} \cdots r_{n-1}$ . But their products  $q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$  are monomials. Explicitly, they can be rewritten as products of the  $r_1, r_2, \dots, r_{n-1}$  using (2). Thus, it is easy to see that the elements of  $\mathcal{Q}'_S$  are the infinite  $\mathbf{k}$ -linear combinations of the monomials  $r_1^{b_1} r_2^{b_2} \cdots r_{n-1}^{b_{n-1}}$  for all  $(b_1, b_2, \dots, b_{n-1}) \in \mathbb{N}^{n-1}$  satisfying  $(b_i \geq b_{i-1} \text{ for all } i \in S)$  and  $(b_i \leq b_{i-1} \text{ for all } i \in [n] \setminus S)$ , where we set  $b_0 = 0$  and  $b_n = 0$ . But we won't need this characterization.)

(e) We let  $\mathcal{Q}_S$  denote the topological  $\mathbf{k}$ -algebra  $\mathbf{k}[[q_i \mid i \in S]]$ . This is a topological subalgebra of  $\mathcal{Q}$ .

(f) We let  $\mathcal{T}_S$  denote the topological  $\mathbf{k}$ -algebra  $\mathbf{k}[[t_i \mid i \in S]]$ . This is a topological subalgebra of  $\mathcal{T}$ .

(g) We define a  $\mathbf{k}$ -algebra homomorphism  $A_S : \mathcal{X}_S \rightarrow \mathcal{Q}'_S$  by

$$A_S(x_{i,j}) = \frac{q_i/q_j}{1 - q_i/q_j} = \sum_{k \geq 0} (q_i/q_j)^k \quad \text{for all } (i,j) \in \mathfrak{P}_S.$$

This is easily seen to be well-defined (because for each  $(i,j) \in \mathfrak{P}_S$  and  $k > 0$ , the  $n$ -tuple  $(0, 0, \dots, 0, k, 0, 0, \dots, 0, -k, 0, 0, \dots, 0)$  (where the  $k$  stands in the  $i$ -th position, and the  $-k$  stands in the  $j$ -th position) is  $S$ -adequate and belongs to  $\mathfrak{Z}$ , and therefore the monomial  $(q_i/q_j)^k$  is in  $\mathcal{Q}'_S$ ).

(h) We define a continuous  $\mathbf{k}$ -linear map  $B_S : \mathcal{Q}'_S \rightarrow \mathcal{Q}_S$  by setting

$$B_S(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{i \in S} q_i^{a_i} \quad \text{for each } S\text{-adequate } (a_1, a_2, \dots, a_n) \in \mathfrak{Z}_S.$$

This is well-defined, as we will see below (in Proposition 2.14 (b)).

(i) We define a continuous  $\mathbf{k}$ -algebra homomorphism  $C_S : \mathcal{Q}_S \rightarrow \mathcal{T}_S$  by

$$C_S(q_i) = \frac{t_i}{1 + t_i} \quad \text{for each } i \in S.$$

This is well-defined, because for each  $i \in S$ , the power series  $\frac{t_i}{1 + t_i}$  has constant term 0 and thus can be substituted into power series.

**Proposition 2.14.** Let  $S$  be a subset of  $[n-1]$ .

(a) We have  $B(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{i \in S} q_i^{a_i}$  for each  $S$ -adequate  $n$ -tuple  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$ .

(b) The map  $B_S$  (defined in Definition 2.13 (h)) is well-defined.

*Proof of Proposition 2.14.* (a) Let  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  be an  $S$ -adequate  $n$ -tuple. We must show that  $B(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{i \in S} q_i^{a_i}$ .

The  $n$ -tuple  $(a_1, a_2, \dots, a_n)$  is  $S$ -adequate. Thus,  $(a_i \geq 0 \text{ for all } i \in S)$  and  $(a_i \leq 0 \text{ for all } i \in [n] \setminus S)$ . In particular,  $(a_i \leq 0 \text{ for all } i \in [n] \setminus S)$ . Hence, each  $i \in [n]$  satisfying  $a_i > 0$  must belong to  $S$  (because otherwise,  $i$  would belong to  $[n] \setminus S$ , and therefore would have to satisfy  $a_i \leq 0$ , which would contradict  $a_i > 0$ ). In particular, each  $i \in [n-1]$  satisfying  $a_i > 0$  must belong to  $S$ .

Now, the definition of the map  $B$  yields

$$B(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{\substack{i \in [n-1]; \\ a_i > 0}} q_i^{a_i} = \prod_{\substack{i \in S; \\ a_i > 0}} q_i^{a_i}$$

(since each  $i \in [n-1]$  satisfying  $a_i > 0$  must belong to  $S$ ). Comparing this with

$$\begin{aligned} \prod_{i \in S} q_i^{a_i} &= \prod_{\substack{i \in S; \\ a_i \geq 0}} q_i^{a_i} \quad (\text{since } a_i \geq 0 \text{ for all } i \in S) \\ &= \left( \prod_{\substack{i \in S; \\ a_i = 0}} \underbrace{q_i^{a_i}}_{=1} \right) \left( \prod_{\substack{i \in S; \\ a_i > 0}} q_i^{a_i} \right) = \prod_{\substack{i \in S; \\ a_i > 0}} q_i^{a_i}, \end{aligned}$$

we obtain  $B(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{i \in S} q_i^{a_i}$ . This proves Proposition 2.14 (a).

(b) We must show that there exists a unique continuous  $\mathbf{k}$ -linear map  $B_S : \mathcal{Q}'_S \rightarrow \mathcal{Q}_S$  satisfying

$$\left( \begin{array}{l} B_S(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{i \in S} q_i^{a_i} \\ \text{for each } S\text{-adequate } (a_1, a_2, \dots, a_n) \in \mathfrak{Z} \end{array} \right). \quad (5)$$

The uniqueness of such a map is clear (because the elements of  $\mathcal{Q}'_S$  are infinite  $\mathbf{k}$ -linear combinations of the monomials  $q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$  for  $S$ -adequate  $n$ -tuples  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$ ; but the formula (5) uniquely determines the value of  $B_S$  on such a  $\mathbf{k}$ -linear combination). Thus, it remains to prove its existence.

For each  $f \in \mathcal{Q}'_S$ , we have  $B(f) \in \mathcal{Q}_S$ <sup>9</sup>. Hence, we can define a map  $\widetilde{B}_S : \mathcal{Q}'_S \rightarrow \mathcal{Q}_S$  by

$$\widetilde{B}_S(f) = B(f) \quad \text{for each } f \in \mathcal{Q}'_S.$$

<sup>9</sup>*Proof.* Let  $f \in \mathcal{Q}'_S$ . We must show that  $B(f) \in \mathcal{Q}_S$ . Since the map  $B$  is  $\mathbf{k}$ -linear and continuous, we can WLOG assume that  $f$  is a monomial of the form  $q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$  for some  $S$ -adequate



This map  $\widetilde{B}_S$  is a restriction of the map  $B$ ; hence, it is a continuous  $\mathbf{k}$ -linear map (since  $B$  is a continuous  $\mathbf{k}$ -linear map). Furthermore, it satisfies

$$\begin{aligned}\widetilde{B}_S(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) &= B(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) \quad (\text{by the definition of } \widetilde{B}_S) \\ &= \prod_{i \in S} q_i^{a_i} \quad (\text{by Proposition 2.14 (a)})\end{aligned}$$

for each  $S$ -adequate  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$ . Hence,  $\widetilde{B}_S$  is a continuous  $\mathbf{k}$ -linear map  $B_S : \mathcal{Q}'_S \rightarrow \mathcal{Q}_S$  satisfying (5). Thus, the existence of such a map  $B_S$  is proven. As we have explained, this completes the proof of Proposition 2.14 (b).  $\square$

**Proposition 2.15.** Let  $S$  be a subset of  $[n - 1]$ . Then, the diagram

$$\begin{array}{ccccccc} \mathcal{X}_S & \xrightarrow{A_S} & \mathcal{Q}'_S & \xrightarrow{B_S} & \mathcal{Q}_S & \xrightarrow{C_S} & \mathcal{T}_S \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathcal{X} & \xrightarrow{A} & \mathcal{Q}' & \xrightarrow{B} & \mathcal{Q} & \xrightarrow{C} & \mathcal{T} \end{array}$$

is commutative.

*Proof of Proposition 2.15.* The commutativity of the left square is obvious<sup>10</sup>. So is

$n$ -tuple  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  (because  $f$  is always an infinite  $\mathbf{k}$ -linear combination of such monomials). Assume this. Consider this  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$ .

Thus,  $f = q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$ . Applying the map  $B$  to both sides of this equality, we obtain

$$\begin{aligned}B(f) &= B(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{i \in S} q_i^{a_i} \quad (\text{by Proposition 2.14 (a)}) \\ &\in \mathcal{Q}_S.\end{aligned}$$

This is precisely what we wanted to show.

<sup>10</sup>“Obvious” in the following sense: You want to prove that a diagram of the form

$$\begin{array}{ccc} \mathcal{A}_1 & \xrightarrow{f_1} & \mathcal{A}_2 \\ f_2 \downarrow & & \downarrow f_3 \\ \mathcal{A}_3 & \xrightarrow{f_4} & \mathcal{A}_4 \end{array}$$

is commutative, where  $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$  are four  $\mathbf{k}$ -algebras and  $f_1, f_2, f_3, f_4$  are four  $\mathbf{k}$ -algebra homomorphisms. (In our concrete case,  $\mathcal{A}_1 = \mathcal{X}_S$ ,  $\mathcal{A}_2 = \mathcal{Q}'_S$ ,  $\mathcal{A}_3 = \mathcal{X}$ ,  $\mathcal{A}_4 = \mathcal{Q}'$ ,  $f_1 = A_S$  and  $f_4 = A$ , whereas  $f_2$  and  $f_3$  are the inclusion maps  $\mathcal{X}_S \rightarrow \mathcal{X}$  and  $\mathcal{Q}'_S \rightarrow \mathcal{Q}'$ .) In order to prove this commutativity, it suffices to show that it holds **on a generating set** of the  $\mathbf{k}$ -algebra  $\mathcal{A}_1$ . In other words, it suffices to pick some generating set  $\mathfrak{G}$  of the  $\mathbf{k}$ -algebra  $\mathcal{A}_1$  and show that all  $g \in \mathfrak{G}$  satisfy  $(f_3 \circ f_1)(g) = (f_4 \circ f_2)(g)$ . (In our concrete case, it is most reasonable to pick  $\mathfrak{G} = \{x_{i,j} \mid (i,j) \in \mathfrak{P}_S\}$ . The proof then becomes completely clear.)

the commutativity of the right square<sup>11</sup>. It thus remains to prove the commutativity of the middle square. In other words, we must show that  $B_S(p) = B(p)$  for each  $p \in \mathcal{Q}'_S$ .

So fix  $p \in \mathcal{Q}'_S$ . Since both maps  $B_S$  and  $B$  are continuous and  $\mathbf{k}$ -linear, we can WLOG assume that  $p$  is a monomial of the form  $q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$  for an  $S$ -adequate  $n$ -tuple  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  (since the elements of  $\mathcal{Q}'_S$  are infinite  $\mathbf{k}$ -linear combinations of monomials of this form). Assume this, and fix this  $(a_1, a_2, \dots, a_n)$ .

From  $p = q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$ , we obtain

$$B(p) = B(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) = \prod_{i \in S} q_i^{a_i} \quad (\text{by Proposition 2.14 (a)}).$$

Comparing this with

$$\begin{aligned} B_S(p) &= B_S(q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) \quad (\text{since } p = q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}) \\ &= \prod_{i \in S} q_i^{a_i} \quad (\text{by the definition of } B_S), \end{aligned}$$

we obtain  $B_S(p) = B(p)$ . This proves the commutativity of the middle square. The proof of Proposition 2.15 is thus complete.  $\square$

**Proposition 2.16.** Let  $S$  be a subset of  $[n-1]$ . Then,  $B_S : \mathcal{Q}'_S \rightarrow \mathcal{Q}_S$  is a continuous  $\mathbf{k}$ -algebra homomorphism.

*Proof of Proposition 2.16.* We merely need to show that  $B_S$  is a  $\mathbf{k}$ -algebra homomorphism. To this purpose, by linearity, we only need to prove that  $B_S(1) = 1$  and  $B_S(mn) = B_S(m)B_S(n)$  for any two monomials  $m$  and  $n$  of the form  $q_1^{a_1} q_2^{a_2} \cdots q_n^{a_n}$  for  $S$ -adequate  $n$ -tuples  $(a_1, a_2, \dots, a_n) \in \mathfrak{Z}$  (since the elements of  $\mathcal{Q}'_S$  are infinite  $\mathbf{k}$ -linear combinations of monomials of this form). This is easy and left to the reader.  $\square$

<sup>11</sup>“Obvious” in the following sense: You want to prove that a diagram of the form

$$\begin{array}{ccc} \mathcal{A}_1 & \xrightarrow{f_1} & \mathcal{A}_2 \\ f_2 \downarrow & & \downarrow f_3 \\ \mathcal{A}_3 & \xrightarrow{f_4} & \mathcal{A}_4 \end{array}$$

is commutative, where  $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$  are four Hausdorff topological  $\mathbf{k}$ -algebras and  $f_1, f_2, f_3, f_4$  are four continuous  $\mathbf{k}$ -algebra homomorphisms. (In our concrete case,  $\mathcal{A}_1 = \mathcal{Q}_S$ ,  $\mathcal{A}_2 = \mathcal{T}_S$ ,  $\mathcal{A}_3 = \mathcal{Q}$ ,  $\mathcal{A}_4 = \mathcal{T}$ ,  $f_1 = C_S$  and  $f_4 = C$ , whereas  $f_2$  and  $f_3$  are the inclusion maps  $\mathcal{Q}_S \rightarrow \mathcal{Q}$  and  $\mathcal{T}_S \rightarrow \mathcal{T}$ .) In order to prove this commutativity, it suffices to show that it holds **on a topological generating set** of the  $\mathbf{k}$ -algebra  $\mathcal{A}_1$ . (A *topological generating set* of a topological  $\mathbf{k}$ -algebra  $\mathcal{A}$  means a subset  $\mathfrak{G}$  of  $\mathcal{A}$  such that the  $\mathbf{k}$ -subalgebra of  $\mathcal{A}$  generated by  $\mathfrak{G}$  is dense in  $\mathcal{A}$ .) In other words, it suffices to pick some topological generating set  $\mathfrak{G}$  of the  $\mathbf{k}$ -algebra  $\mathcal{A}_1$  and show that all  $g \in \mathfrak{G}$  satisfy  $(f_3 \circ f_1)(g) = (f_4 \circ f_2)(g)$ . (In our concrete case, it is most reasonable to pick  $\mathfrak{G} = \{q_i \mid i \in S\}$ . The proof then becomes completely clear.)

**Proposition 2.17.** Let  $S$  be a subset of  $[n - 1]$ . Let  $(i, j) \in \mathfrak{P}_S$ . Then,

$$(B_S \circ A_S)(x_{i,j}) = \frac{q_i}{1 - q_i}.$$

*Proof of Proposition 2.17.* From  $(i, j) \in \mathfrak{P}_S$ , we obtain  $i \in S$  and  $j \in [n] \setminus S$ , so that  $j \notin S$ . From this, it becomes clear that  $B_S(q_i/q_j) = q_i$  (by the definition of  $B_S$ ).

Proposition 2.16 shows that  $B_S : \mathcal{Q}'_S \rightarrow \mathcal{Q}_S$  is a continuous  $\mathbf{k}$ -algebra homomorphism. Now,

$$\begin{aligned} (B_S \circ A_S)(x_{i,j}) &= B_S \left( \frac{\underbrace{A_S(x_{i,j})}_{= \frac{q_i/q_j}{1 - q_i/q_j}}}{1 - q_i/q_j} \right) = B_S \left( \frac{q_i/q_j}{1 - q_i/q_j} \right) = \frac{B_S(q_i/q_j)}{1 - B_S(q_i/q_j)} \\ &\quad \left( \begin{array}{l} \text{since } B_S \text{ is a continuous } \mathbf{k}\text{-algebra homomorphism,} \\ \text{and thus commutes with any power series} \end{array} \right) \\ &= \frac{q_i}{1 - q_i} \quad (\text{since } B_S(q_i/q_j) = q_i). \end{aligned}$$

This proves Proposition 2.17.  $\square$

**Proposition 2.18.** Let  $\mathfrak{m} \in \mathfrak{M}$  be a pathless monomial.

- (a) There exists a subset  $S$  of  $[n - 1]$  such that  $\mathfrak{m}$  is  $S$ -friendly.
- (b) Let  $S$  be such a subset. Then,  $\mathfrak{m} \in \mathcal{X}_S$  and  $D(\mathfrak{m}) = (C_S \circ B_S \circ A_S)(\mathfrak{m})$ .

*Proof of Proposition 2.18.* (a) Write  $\mathfrak{m}$  in the form  $\mathfrak{m} = \prod_{\substack{(i,j) \in [n]^2; \\ i < j}} x_{i,j}^{a_{i,j}}$ . For each  $i \in$

$[n - 1]$ , define a  $b_i \in \mathbb{N}$  by  $b_i = \sum_{j=i+1}^n a_{i,j}$ . Define a subset  $S$  of  $[n - 1]$  by  $S = \{i \in [n - 1] \mid b_i > 0\}$ . Then  $\mathfrak{m}$  is  $S$ -friendly<sup>12</sup>. This proves Proposition 2.18 (a).

<sup>12</sup>*Proof.* We need to show that every indeterminate  $x_{i,j}$  that appears in  $\mathfrak{m}$  satisfies  $i \in S$  and  $j \notin S$ .

Indeed, assume the contrary. Thus, some indeterminate  $x_{i,j}$  that appears in  $\mathfrak{m}$  does **not** satisfy  $i \in S$  and  $j \notin S$ . Fix such an indeterminate  $x_{i,j}$ , and denote it by  $x_{u,v}$ . Thus,  $x_{u,v}$  is an indeterminate that appears in  $\mathfrak{m}$  but does **not** satisfy  $u \in S$  and  $v \notin S$ . Therefore, we have either  $u \notin S$  or  $v \in S$  (or both).

We have  $1 \leq u < v \leq n$  (since the indeterminate  $x_{u,v}$  exists) and thus  $u \in [n - 1]$ . The definition of  $b_u$  yields  $b_u = \sum_{j=u+1}^n a_{u,j}$ . But  $v \geq u + 1$  (since  $u < v$ ). Hence,  $a_{u,v}$  is an addend of the sum  $\sum_{j=u+1}^n a_{u,j}$ . Hence,  $\sum_{j=u+1}^n a_{u,j} \geq a_{u,v}$ . But  $a_{u,v} > 0$  (since the indeterminate  $x_{u,v}$

(b) We know that  $\mathfrak{m} \in \mathcal{X}_S$  (since  $\mathfrak{m}$  is  $S$ -friendly). Now, we shall show that  $D|_{\mathcal{X}_S} = C_S \circ B_S \circ A_S$  (if we regard  $C_S \circ B_S \circ A_S$  as a map to  $\mathcal{T}$ ).

The map  $D|_{\mathcal{X}_S}$  is a  $\mathbf{k}$ -algebra homomorphism (since  $D$  is a  $\mathbf{k}$ -algebra homomorphism), and the map  $C_S \circ B_S \circ A_S$  is a  $\mathbf{k}$ -algebra homomorphism (since all of  $C_S$ ,  $B_S$  and  $A_S$  are  $\mathbf{k}$ -algebra homomorphisms<sup>13</sup>). Hence, we are trying to prove that two  $\mathbf{k}$ -algebra homomorphisms are equal (namely, the homomorphisms  $D|_{\mathcal{X}_S}$  and  $C_S \circ B_S \circ A_S$ ). It is clearly enough to prove this on the generating family  $(x_{i,j})_{(i,j) \in \mathfrak{P}_S}$  of the  $\mathbf{k}$ -algebra  $\mathcal{X}_S$ . In other words, it is enough to prove that  $(D|_{\mathcal{X}_S})(x_{i,j}) = (C_S \circ B_S \circ A_S)(x_{i,j})$  for each  $(i,j) \in \mathfrak{P}_S$ .

So let us fix some  $(i,j) \in \mathfrak{P}_S$ . Then,  $(D|_{\mathcal{X}_S})(x_{i,j}) = D(x_{i,j}) = t_i$  (by the definition of  $D$ ). Comparing this with

$$\begin{aligned} (C_S \circ B_S \circ A_S)(x_{i,j}) &= C_S \left( \underbrace{(B_S \circ A_S)(x_{i,j})}_{\substack{= \frac{q_i}{1-q_i} \\ \text{(by Proposition 2.17)}}} \right) = C_S \left( \frac{q_i}{1-q_i} \right) = \frac{C_S(q_i)}{1-C_S(q_i)} \\ &\quad \left( \begin{array}{c} \text{because the map } C_S \text{ is a continuous } \mathbf{k}\text{-algebra} \\ \text{homomorphism, and thus} \\ \text{commutes with any power series} \end{array} \right) \\ &= \frac{\left( \frac{t_i}{1+t_i} \right)}{1 - \frac{t_i}{1+t_i}} \quad \left( \text{since } C_S(q_i) = \frac{t_i}{1+t_i} \right) \\ &= t_i, \end{aligned}$$

we obtain  $(D|_{\mathcal{X}_S})(x_{i,j}) = (C_S \circ B_S \circ A_S)(x_{i,j})$ .

This completes our proof of  $D|_{\mathcal{X}_S} = C_S \circ B_S \circ A_S$ . Now, from  $\mathfrak{m} \in \mathcal{X}_S$ , we

---

appears in  $\mathfrak{m}$ ). Hence,  $b_u = \sum_{j=u+1}^n a_{u,j} \geq a_{u,v} > 0$ . Therefore,  $u \in S$  (by the definition of  $S$ ).

Hence,  $u \notin S$  cannot hold. Therefore,  $v \in S$  (since we know that we have either  $u \notin S$  or  $v \in S$ ). In other words,  $v \in [n-1]$  and  $b_v > 0$  (by the definition of  $S$ ). But the definition of  $b_v$  yields  $b_v = \sum_{j=v+1}^n a_{v,j} = \sum_{w=v+1}^n a_{v,w}$ . Hence,  $\sum_{w=v+1}^n a_{v,w} = b_v > 0$ . Hence, there exists some  $w \in \{v+1, v+2, \dots, n\}$  such that  $a_{v,w} > 0$ . Fix such a  $w$ .

We have  $v < w$  (since  $w \in \{v+1, v+2, \dots, n\}$ ), hence  $u < v < w$ . Thus,  $(u, v) \neq (v, w)$ . Moreover, the indeterminate  $x_{v,w}$  appears in  $\mathfrak{m}$  (since  $a_{v,w} > 0$ ). Thus, both indeterminates  $x_{u,v}$  and  $x_{v,w}$  appear in  $\mathfrak{m}$ . Hence,  $x_{u,v}x_{v,w} \mid \mathfrak{m}$  (since  $(u, v) \neq (v, w)$ ).

But the monomial  $\mathfrak{m}$  is pathless. In other words, there exists no triple  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$  and  $x_{i,j}x_{j,k} \mid \mathfrak{m}$ . This contradicts the fact that  $(u, v, w)$  is such a triple (since  $u < v < w$  and  $x_{u,v}x_{v,w} \mid \mathfrak{m}$ ). This contradiction completes our proof.

<sup>13</sup>Here we are using Proposition 2.16.

obtain  $D(\mathfrak{m}) = \underbrace{(D|_{\mathcal{X}_S})}_{=C_S \circ B_S \circ A_S}(\mathfrak{m}) = (C_S \circ B_S \circ A_S)(\mathfrak{m})$ . This completes the proof of Proposition 2.18 (b).  $\square$

## 2.9. $D(q) = (C \circ B \circ A)(q)$ for pathless $q$

**Corollary 2.19.** Let  $q \in \mathcal{X}$  be pathless. Then,  $D(q) = (C \circ B \circ A)(q)$ .

*Proof of Corollary 2.19.* The polynomial  $q$  is pathless, i.e., is a  $\mathbf{k}$ -linear combination of pathless monomials. Hence, we WLOG assume that  $q$  is a pathless monomial  $\mathfrak{m}$  (since both maps  $D$  and  $C \circ B \circ A$  are  $\mathbf{k}$ -linear). Consider this  $\mathfrak{m}$ .

Proposition 2.18 (a) shows that there exists a subset  $S$  of  $[n-1]$  such that  $\mathfrak{m}$  is  $S$ -friendly. Consider this  $S$ .

Proposition 2.18 (b) yields  $\mathfrak{m} \in \mathcal{X}_S$  and  $D(\mathfrak{m}) = (C_S \circ B_S \circ A_S)(\mathfrak{m})$ . But the commutativity of the diagram in Proposition 2.15 shows that  $C_S \circ B_S \circ A_S = (C \circ B \circ A)|_{\mathcal{X}_S}$  (provided that we regard  $C_S \circ B_S \circ A_S$  as a map to  $\mathcal{T}$ ). Hence,

$$\underbrace{(C_S \circ B_S \circ A_S)}_{=(C \circ B \circ A)|_{\mathcal{X}_S}}(\mathfrak{m}) = ((C \circ B \circ A)|_{\mathcal{X}_S})(\mathfrak{m}) = (C \circ B \circ A)(\mathfrak{m}).$$

Thus,  $D(\mathfrak{m}) = (C_S \circ B_S \circ A_S)(\mathfrak{m}) = (C \circ B \circ A)(\mathfrak{m})$ . Since  $q = \mathfrak{m}$ , this rewrites as  $D(q) = (C \circ B \circ A)(q)$ . This proves Corollary 2.19.  $\square$

## 2.10. Proof of Theorem 1.7 for $\beta = 1$

**Lemma 2.20.** Let  $p \in \mathcal{X}$  be a pathless polynomial such that  $p \in \mathcal{J}_1$ . Then,  $D(p) = 0$ .

*Proof of Lemma 2.20.* We have  $A\left(\underbrace{p}_{\in \mathcal{J}_1}\right) \in A(\mathcal{J}_1) = 0$  (by Proposition 2.5); thus,  $A(p) = 0$ . But Corollary 2.19 (applied to  $q = p$ ) yields

$$D(p) = (C \circ B \circ A)(p) = (C \circ B)\left(\underbrace{A(p)}_{=0}\right) = (C \circ B)(0) = 0$$

(since the map  $C \circ B$  is  $\mathbf{k}$ -linear). This proves Lemma 2.20.  $\square$

We are now ready to prove Theorem 1.7 in the case  $\beta = 1$ :

**Lemma 2.21.** Let  $p \in \mathcal{X}$ . Consider any pathless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_1}$ . Then,  $D(q)$  does not depend on the choice of  $q$  (but merely on the choice of  $p$ ).

*Proof of Lemma 2.21.* We need to prove that  $D(q)$  does not depend on the choice of  $q$ . In other words, we need to prove that if  $f$  and  $g$  are two pathless polynomials  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_1}$ , then  $D(f) = D(g)$ .

So let  $f$  and  $g$  be two pathless polynomials  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_1}$ . Thus,  $p \equiv f \pmod{\mathcal{J}_1}$  and  $p \equiv g \pmod{\mathcal{J}_1}$ . Hence,  $f \equiv p \equiv g \pmod{\mathcal{J}_1}$ , so that  $f - g \in \mathcal{J}_1$ . Also, the polynomial  $f - g \in \mathcal{X}$  is pathless (since it is the difference of the two pathless polynomials  $f$  and  $g$ ). Thus, Lemma 2.20 (applied to  $f - g$  instead of  $p$ ) shows that  $D(f - g) = 0$ . Thus,  $0 = D(f - g) = D(f) - D(g)$  (since  $D$  is a  $\mathbf{k}$ -algebra homomorphism). In other words,  $D(f) = D(g)$ . This proves Lemma 2.21.  $\square$

## 2.11. Proof of Theorem 1.7 for $\beta$ regular

Let us now state a simple lemma:

**Lemma 2.22.** Let  $\beta$  be a regular element of  $\mathbf{k}$ . Define a  $\mathbf{k}$ -algebra homomorphism  $G : \mathcal{T}' \rightarrow \mathcal{T}'$  by

$$G(t_i) = \beta t_i \quad \text{for all } i \in [n-1].$$

This map  $G$  is injective.

*Proof of Lemma 2.22.* Let  $\mathfrak{T}$  denote the set of all monomials in the indeterminates  $t_1, t_2, \dots, t_{n-1}$ . It is easy to see that

$$G(t) = \beta^{\deg t} t \quad \text{for each monomial } t \in \mathfrak{T}. \quad (6)$$

Now, let  $f \in \text{Ker } G$ . Then,  $f \in \mathcal{T}'$ . Hence, we can write  $f$  in the form  $f = \sum_{t \in \mathfrak{T}} \lambda_t t$  for some family  $(\lambda_t)_{t \in \mathfrak{T}} \in \mathbf{k}^{\mathfrak{T}}$  (since every polynomial in  $\mathcal{T}'$  is a  $\mathbf{k}$ -linear combination of the monomials  $t \in \mathfrak{T}$ ). Consider this family  $(\lambda_t)_{t \in \mathfrak{T}}$ .

From  $f \in \text{Ker } G$ , we obtain  $G(f) = 0$ . Thus,

$$\begin{aligned} 0 &= G(f) = G\left(\sum_{t \in \mathfrak{T}} \lambda_t t\right) \quad \left(\text{since } f = \sum_{t \in \mathfrak{T}} \lambda_t t\right) \\ &= \sum_{t \in \mathfrak{T}} \lambda_t \underbrace{G(t)}_{\substack{= \beta^{\deg t} t \\ \text{(by (6))}}} \quad (\text{since the map } G \text{ is } \mathbf{k}\text{-linear}) \\ &= \sum_{t \in \mathfrak{T}} \lambda_t \beta^{\deg t} t = \sum_{t \in \mathfrak{T}} \beta^{\deg t} \lambda_t t. \end{aligned}$$

In other words,  $\sum_{t \in \mathfrak{T}} \beta^{\deg t} \lambda_t t = 0$ . Since the monomials  $t \in \mathfrak{T}$  in  $\mathcal{T}'$  are  $\mathbf{k}$ -linearly independent, we thus obtain

$$\beta^{\deg t} \lambda_t = 0 \quad \text{for each } t \in \mathfrak{T}. \quad (7)$$

Thus, we can easily obtain  $\lambda_t = 0$  for each  $t \in \mathfrak{T}$ <sup>14</sup>. Hence,  $\sum_{t \in \mathfrak{T}} \underbrace{\lambda_t}_{=0} t = \sum_{t \in \mathfrak{T}} 0t = 0$ , so that  $f = \sum_{t \in \mathfrak{T}} \lambda_t t = 0$ .

Now, forget that we fixed  $f$ . We thus have shown that  $f = 0$  for each  $f \in \text{Ker } G$ . In other words,  $\text{Ker } G = 0$ . Hence, the map  $G$  is injective (since  $G$  is  $\mathbf{k}$ -linear). This proves Lemma 2.22.  $\square$

The following lemma generalizes Lemma 2.20:

**Lemma 2.23.** Let  $\beta$  be a regular element of  $\mathbf{k}$ . Let  $p \in \mathcal{X}$  be a pathless polynomial such that  $p \in \mathcal{J}_\beta$ . Then,  $D(p) = 0$ .

*Proof of Lemma 2.23.* Define a  $\mathbf{k}$ -algebra homomorphism  $F : \mathcal{X} \rightarrow \mathcal{X}$  by

$$F(x_{i,j}) = \beta x_{i,j} \quad \text{for all } (i,j) \in [n]^2 \text{ satisfying } i < j.$$

Define a  $\mathbf{k}$ -algebra homomorphism  $G : \mathcal{T}' \rightarrow \mathcal{T}'$  by

$$G(t_i) = \beta t_i \quad \text{for all } i \in [n-1].$$

Lemma 2.22 shows that this map  $G$  is injective. Hence,  $\text{Ker } G = 0$ .

A trivial computation shows that the diagram

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{D} & \mathcal{T}' \\ F \downarrow & & \downarrow G \\ \mathcal{X} & \xrightarrow{D} & \mathcal{T}' \end{array}$$

is commutative. In other words,  $D \circ F = G \circ D$ .

It is easy to check that  $F(\mathcal{J}_\beta) \subseteq \mathcal{J}_1$ . (Indeed, the  $\mathbf{k}$ -algebra homomorphism  $F$  sends each generator  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta)$  of  $\mathcal{J}_\beta$  to

$$(\beta x_{i,j})(\beta x_{j,k}) - (\beta x_{i,k})(\beta x_{i,j} + \beta x_{j,k} + \beta) = \beta^2 \underbrace{(x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + 1))}_{\substack{\in \mathcal{J}_1 \\ \text{(since the ideal } \mathcal{J}_1 \text{ is generated} \\ \text{by polynomials like this)}}} \in \mathcal{J}_1.$$

)

It is easy to see (using the definition of  $F$ ) that  $F(m) = \beta^{\deg m} m$  for each monomial  $m \in \mathfrak{M}$ . Hence, the map  $F$  sends each pathless monomial  $m \in \mathfrak{M}$  to a scalar multiple of a pathless monomial (namely, to  $\beta^{\deg m} m$ ). Thus, the map  $F$  sends pathless polynomials to pathless polynomials. Therefore,  $F(p) \in \mathcal{X}$

<sup>14</sup>*Proof.* Let  $t \in \mathfrak{T}$ . From (7), we obtain  $\beta^{\deg t} \lambda_t = 0$ .

Recall that the element  $\beta$  of  $\mathbf{k}$  is regular. Hence, its power  $\beta^{\deg t}$  is regular as well. Thus, from  $\beta^{\deg t} \lambda_t = 0$ , we obtain  $\lambda_t = 0$ . Qed.

is pathless (since  $p \in \mathcal{X}$  is pathless). Also,  $F \left( \underbrace{p}_{\in \mathcal{J}_\beta} \right) \in F(\mathcal{J}_\beta) \subseteq \mathcal{J}_1$ . Thus,

Lemma 2.20 (applied to  $F(p)$  instead of  $p$ ) shows that  $D(F(p)) = 0$ . Since

$$D(F(p)) = \underbrace{(D \circ F)(p)}_{=G \circ D} = (G \circ D)(p) = G(D(p)),$$

this rewrites as  $G(D(p)) = 0$ . Hence,  $D(p) \in \text{Ker } G = 0$ , so that  $D(p) = 0$ . This proves Lemma 2.23.  $\square$

As a consequence, we obtain a further particular case of Theorem 1.7:

**Proposition 2.24.** Let  $\beta$  be a regular element of  $\mathbf{k}$ . Let  $p \in \mathcal{X}$ . Consider any pathless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_\beta}$ . Then,  $D(q)$  does not depend on the choice of  $q$  (but merely on the choice of  $\beta$  and  $p$ ).

*Proof of Proposition 2.24.* Proposition 2.24 follows from Lemma 2.23 in the same way as we derived Lemma 2.21 from Lemma 2.20 (with the only difference that  $\mathcal{J}_1$  is replaced by  $\mathcal{J}_\beta$  throughout the proof).  $\square$

## 2.12. Proof of Theorem 1.7 for all $\beta$

Let us now prepare for the final steps of our way to Theorem 1.7.

**Definition 2.25.** Fix any element  $\beta \in \mathbf{k}$ .

(a) Let  $\mathbf{m}$  be the polynomial ring  $\mathbf{k}[b]$  in one indeterminate  $b$  over  $\mathbf{k}$ .

(b) Let  $\pi : \mathbf{m} \rightarrow \mathbf{k}$  be the unique  $\mathbf{k}$ -algebra homomorphism from  $\mathbf{k}[b]$  to  $\mathbf{k}$  that sends  $b$  to  $\beta$ . (This is well-defined by the universal property of the polynomial ring  $\mathbf{k}[b] = \mathbf{m}$ .) In other words,  $\pi$  is the evaluation map that sends each polynomial  $f \in \mathbf{k}[b]$  to its evaluation  $f(\beta)$  at  $\beta$ . It is easy to see that  $\text{Ker } \pi = (b - \beta) \mathbf{m}$ .

(c) Let  $\mathcal{X}^{[\mathbf{m}]}$  be the polynomial ring  $\mathbf{m}[x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j]$ . In other words,  $\mathcal{X}^{[\mathbf{m}]}$  is the  $\mathbf{m}$ -algebra that is defined in the same way as  $\mathcal{X}$  but using the base ring  $\mathbf{m}$  instead of  $\mathbf{k}$ .

(d) Let  $\mathcal{T}'^{[\mathbf{m}]}$  be the polynomial ring  $\mathbf{m}[t_1, t_2, \dots, t_{n-1}]$ . In other words,  $\mathcal{T}'^{[\mathbf{m}]}$  is the  $\mathbf{m}$ -algebra that is defined in the same way as  $\mathcal{T}'$  but using the base ring  $\mathbf{m}$  instead of  $\mathbf{k}$ .

(e) Let  $D^{[\mathbf{m}]} : \mathcal{X}^{[\mathbf{m}]} \rightarrow \mathcal{T}'^{[\mathbf{m}]}$  be the  $\mathbf{m}$ -algebra homomorphism defined in the same way as the  $\mathbf{k}$ -algebra homomorphism  $D : \mathcal{X} \rightarrow \mathcal{T}'$  but using the base ring  $\mathbf{m}$  instead of  $\mathbf{k}$ .

(f) The  $\mathbf{k}$ -algebra homomorphism  $\pi : \mathbf{m} \rightarrow \mathbf{k}$  induces a  $\mathbf{k}$ -algebra homomorphism

$$\mathbf{m}[x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j] \rightarrow \mathbf{k}[x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j]$$



which sends each  $f \in \mathbf{m}$  to  $\pi(f)$  while sending each indeterminate  $x_{i,j}$  to the corresponding indeterminate  $x_{i,j}$ . This latter homomorphism will be denoted by  $\pi^{\mathcal{X}}$ . Notice that  $\pi^{\mathcal{X}}$  is a  $\mathbf{k}$ -algebra homomorphism from  $\mathcal{X}^{[\mathbf{m}]}$  to  $\mathcal{X}$  (since  $\mathbf{m} \left[ x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j \right] = \mathcal{X}^{[\mathbf{m}]}$  and  $\mathbf{k} \left[ x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j \right] = \mathcal{X}$ ).

Explicitly speaking, the homomorphism  $\pi^{\mathcal{X}}$  acts on a polynomial  $f \in \mathcal{X}^{[\mathbf{m}]}$  by applying the map  $\pi$  to each of its coefficients.

(g) The  $\mathbf{k}$ -algebra homomorphism  $\pi : \mathbf{m} \rightarrow \mathbf{k}$  induces a  $\mathbf{k}$ -algebra homomorphism

$$\mathbf{m} [t_1, t_2, \dots, t_{n-1}] \rightarrow \mathbf{k} [t_1, t_2, \dots, t_{n-1}]$$

which sends each  $f \in \mathbf{m}$  to  $\pi(f)$  while sending each indeterminate  $t_i$  to the corresponding indeterminate  $t_i$ . This latter homomorphism will be denoted by  $\pi^{\mathcal{T}'}$ . Notice that  $\pi^{\mathcal{T}'}$  is a  $\mathbf{k}$ -algebra homomorphism from  $\mathcal{T}'^{[\mathbf{m}]}$  to  $\mathcal{T}'$  (since  $\mathbf{m} [t_1, t_2, \dots, t_{n-1}] = \mathcal{T}'^{[\mathbf{m}]}$  and  $\mathbf{k} [t_1, t_2, \dots, t_{n-1}] = \mathcal{T}'$ ).

Explicitly speaking, the homomorphism  $\pi^{\mathcal{T}'}$  acts on a polynomial  $f \in \mathcal{T}'^{[\mathbf{m}]}$  by applying the map  $\pi$  to each of its coefficients.

(h) Let  $\mathcal{J}_b^{[\mathbf{m}]}$  be the ideal of  $\mathcal{X}^{[\mathbf{m}]}$  defined in the same way as  $\mathcal{J}_\beta$  but using the base ring  $\mathbf{m}$  and the element  $b \in \mathbf{m}$  instead of the base ring  $\mathbf{k}$  and the element  $\beta \in \mathbf{k}$ .

We notice some simple facts:

**Lemma 2.26. (a)** The element  $b$  of  $\mathbf{m}$  is regular.

(b) We have  $\mathcal{J}_\beta = \pi^{\mathcal{X}} \left( \mathcal{J}_b^{[\mathbf{m}]} \right)$ .

(c) For every pathless polynomial  $f \in \mathcal{X}$ , there exists a pathless polynomial  $g \in \mathcal{X}^{[\mathbf{m}]}$  satisfying  $f = \pi^{\mathcal{X}}(g)$ .

(d) We have  $\text{Ker}(\pi^{\mathcal{X}}) = (b - \beta) \mathcal{X}^{[\mathbf{m}]}$ .

(e) We have  $\pi^{\mathcal{T}'} \circ D^{[\mathbf{m}]} = D \circ \pi^{\mathcal{X}}$ .

*Proof of Lemma 2.26. (a)* This is clear, since  $b$  is the indeterminate in the polynomial ring  $\mathbf{k}[b]$ .

(b) The  $\mathbf{k}$ -algebra homomorphism  $\pi : \mathbf{m} \rightarrow \mathbf{k}$  is surjective (since the canonical inclusion map  $\iota : \mathbf{k} \rightarrow \mathbf{m}$  satisfies  $\pi \circ \iota = \text{id}$ ). Hence, the  $\mathbf{k}$ -algebra homomorphism

$$\pi^{\mathcal{X}} : \mathbf{m} \left[ x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j \right] \rightarrow \mathbf{k} \left[ x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j \right]$$

induced by  $\pi$  is surjective as well. Since  $\mathbf{m} \left[ x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j \right] = \mathcal{X}^{[\mathbf{m}]}$  and  $\mathbf{k} \left[ x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j \right] = \mathcal{X}$ , this rewrites as follows:

The  $\mathbf{k}$ -algebra homomorphism  $\pi^{\mathcal{X}} : \mathcal{X}^{[\mathbf{m}]} \rightarrow \mathcal{X}$  is surjective<sup>15</sup>. Hence,  $\pi^{\mathcal{X}} \left( \mathcal{X}^{[\mathbf{m}]} \right) = \mathcal{X}$ .

<sup>15</sup>In fact, slightly more holds: Let  $\iota : \mathbf{k} \rightarrow \mathbf{m}$  be the canonical inclusion map.

Let  $J_\beta$  be the  $\mathbb{Z}$ -submodule of  $\mathcal{X}$  spanned by all elements of the form  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta)$  for  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$ . Then, the ideal  $\mathcal{J}_\beta$  of  $\mathcal{X}$  is generated by this  $\mathbb{Z}$ -submodule  $J_\beta$  (since  $\mathcal{J}_\beta$  is generated by all elements of this form). Thus,  $\mathcal{J}_\beta = \mathcal{X}J_\beta$  (a product of two  $\mathbb{Z}$ -submodules of  $\mathcal{X}$ ).

Let  $J_b$  be the  $\mathbb{Z}$ -submodule of  $\mathcal{X}^{[\mathbf{m}]}$  spanned by all elements of the form  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + b)$  for  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$ . Then, the ideal  $\mathcal{J}_b^{[\mathbf{m}]}$  of  $\mathcal{X}^{[\mathbf{m}]}$  is generated by this  $\mathbb{Z}$ -submodule  $J_b$  (since  $\mathcal{J}_b^{[\mathbf{m}]}$  is generated by all elements of this form). Thus,  $\mathcal{J}_b^{[\mathbf{m}]} = \mathcal{X}^{[\mathbf{m}]}J_b$  (a product of two  $\mathbb{Z}$ -submodules of  $\mathcal{X}^{[\mathbf{m}]}$ ).

For each  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$ , we have

$$\begin{aligned} & \pi^{\mathcal{X}}(x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + b)) \\ &= x_{i,j}x_{j,k} - x_{i,k}\left(x_{i,j} + x_{j,k} + \underbrace{\pi(b)}_{=\beta}\right) \quad \left(\text{by the definition of the map } \pi^{\mathcal{X}}\right) \\ &= x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta). \end{aligned}$$

Thus, the map  $\pi^{\mathcal{X}}$  sends each of the designated generators of the  $\mathbb{Z}$ -module  $J_b$  to the corresponding generator of the  $\mathbb{Z}$ -module  $J_\beta$ . Therefore,  $\pi^{\mathcal{X}}(J_b) = J_\beta$  (since the map  $\pi^{\mathcal{X}}$  is  $\mathbb{Z}$ -linear).

Now,

$$\begin{aligned} \pi^{\mathcal{X}}\left(\underbrace{\mathcal{J}_b^{[\mathbf{m}]}}_{=\mathcal{X}^{[\mathbf{m}]}J_b}\right) &= \pi^{\mathcal{X}}(\mathcal{X}^{[\mathbf{m}]}J_b) \\ &= \underbrace{\pi^{\mathcal{X}}(\mathcal{X}^{[\mathbf{m}]})}_{=\mathcal{X}} \underbrace{\pi^{\mathcal{X}}(J_b)}_{=J_\beta} \quad \left(\text{since } \pi^{\mathcal{X}} \text{ is a ring homomorphism}\right) \\ &= \mathcal{X}J_\beta = \mathcal{J}_\beta. \end{aligned}$$

This proves Lemma 2.26 (b).

(c) For the purpose of this proof, we shall regard  $\mathbf{k}$  as a  $\mathbf{k}$ -subalgebra of  $\mathbf{m}$  via the canonical inclusion  $\mathbf{k} \rightarrow \mathbf{m}$  (sending each  $\lambda \in \mathbf{k}$  to the constant polynomial  $\lambda \in \mathbf{m}$ ). Then,  $\mathcal{X}$  also becomes a  $\mathbf{k}$ -subalgebra of  $\mathcal{X}^{[\mathbf{m}]}$ . Moreover, it is fairly clear that  $\pi^{\mathcal{X}}(f) = f$  for each  $f \in \mathcal{X}$  (because  $\pi(\lambda) = \lambda$  for each  $\lambda \in \mathbf{k}$ ).

Now, let  $f \in \mathcal{X}$  be a pathless polynomial. Then,  $f$ , when considered as a polynomial in  $\mathcal{X}^{[\mathbf{m}]}$ , is still a pathless polynomial. Moreover,  $\pi^{\mathcal{X}}(f) = f$ . Thus,

---

Let  $\iota^{\mathcal{X}}$  denote the  $\mathbf{k}$ -algebra homomorphism  $\mathbf{k}[x_{i,j} \mid (i, j) \in [n]^2 \text{ satisfying } i < j] \rightarrow \mathbf{m}[x_{i,j} \mid (i, j) \in [n]^2 \text{ satisfying } i < j]$  induced by this  $\mathbf{k}$ -algebra homomorphism  $\iota$ . Then, from  $\pi \circ \iota = \text{id}$ , we easily obtain  $\pi^{\mathcal{X}} \circ \iota^{\mathcal{X}} = \text{id}$  (by functoriality). Hence,  $\pi^{\mathcal{X}}$  is surjective.

---

there exists a pathless polynomial  $g \in \mathcal{X}^{[\mathbf{m}]}$  satisfying  $f = \pi^{\mathcal{X}}(g)$  (namely,  $g = f$ ). This proves Lemma 2.26 (c).

(d) Let  $p \in \text{Ker}(\pi^{\mathcal{X}})$ . Thus,  $p \in \mathcal{X}^{[\mathbf{m}]}$ . Write  $p$  in the form  $p = \sum_{\mathbf{m} \in \mathfrak{M}} f_{\mathbf{m}} \mathbf{m}$  for some family  $(f_{\mathbf{m}})_{\mathbf{m} \in \mathfrak{M}} \in \mathbf{m}^{\mathfrak{M}}$ . (This is possible, since every polynomial in  $\mathcal{X}^{[\mathbf{m}]}$  is a unique  $\mathbf{m}$ -linear combination of the monomials  $\mathbf{m} \in \mathfrak{M}$ .) Applying the map  $\pi^{\mathcal{X}}$  to the equality  $p = \sum_{\mathbf{m} \in \mathfrak{M}} f_{\mathbf{m}} \mathbf{m}$ , we obtain

$$\pi^{\mathcal{X}}(p) = \pi^{\mathcal{X}}\left(\sum_{\mathbf{m} \in \mathfrak{M}} f_{\mathbf{m}} \mathbf{m}\right) = \sum_{\mathbf{m} \in \mathfrak{M}} \pi(f_{\mathbf{m}}) \mathbf{m} \quad (8)$$

(by the definition of  $\pi^{\mathcal{X}}$ ).

Recall that  $p \in \text{Ker}(\pi^{\mathcal{X}})$ . Thus,  $\pi^{\mathcal{X}}(p) = 0$ . In view of (8), this rewrites as  $\sum_{\mathbf{m} \in \mathfrak{M}} \pi(f_{\mathbf{m}}) \mathbf{m} = 0$ . Since the monomials  $\mathbf{m} \in \mathfrak{M}$  in  $\mathcal{X}$  are  $\mathbf{k}$ -linearly independent, this shows that  $\pi(f_{\mathbf{m}}) = 0$  for each  $\mathbf{m} \in \mathfrak{M}$ . Thus, for each  $\mathbf{m} \in \mathfrak{M}$ , we have  $f_{\mathbf{m}} \in \text{Ker} \pi = (b - \beta) \mathbf{m}$ . Hence,

$$p = \sum_{\mathbf{m} \in \mathfrak{M}} \underbrace{f_{\mathbf{m}}}_{\in (b-\beta)\mathbf{m}} \mathbf{m} \in \sum_{\mathbf{m} \in \mathfrak{M}} (b - \beta) \underbrace{\mathbf{m}\mathbf{m}}_{\subseteq \mathcal{X}^{[\mathbf{m}]}} \subseteq (b - \beta) \mathcal{X}^{[\mathbf{m}]}.$$

Now, forget that we fixed  $p$ . We thus have shown that  $p \in (b - \beta) \mathcal{X}^{[\mathbf{m}]}$  for each  $p \in \text{Ker}(\pi^{\mathcal{X}})$ . In other words,  $\text{Ker}(\pi^{\mathcal{X}}) \subseteq (b - \beta) \mathcal{X}^{[\mathbf{m}]}$ .

Observe that  $b - \beta \in (b - \beta) \mathbf{m} = \text{Ker} \pi$ , and thus  $\pi(b - \beta) = 0$ .

On the other hand, let us regard  $\mathbf{m}$  as a subring of the polynomial ring  $\mathcal{X}^{[\mathbf{m}]}$ . Then,  $\pi^{\mathcal{X}}(f)$  is well-defined for each  $f \in \mathbf{m}$  (since  $f \in \mathbf{m} \subseteq \mathcal{X}^{[\mathbf{m}]}$ ). Furthermore, each  $f \in \mathbf{m}$  satisfies  $\pi^{\mathcal{X}}(f) = \pi(f)$  (by the definition of  $\pi^{\mathcal{X}}$ ). Applying this to  $f = b - \beta$ , we obtain  $\pi^{\mathcal{X}}(b - \beta) = \pi(b - \beta) = 0$ .

But  $\pi^{\mathcal{X}}$  is a  $\mathbf{k}$ -algebra homomorphism. Hence,

$$\pi^{\mathcal{X}}\left((b - \beta) \mathcal{X}^{[\mathbf{m}]}\right) = \underbrace{\pi^{\mathcal{X}}(b - \beta)}_{=0} \pi^{\mathcal{X}}\left(\mathcal{X}^{[\mathbf{m}]}\right) = 0 \pi^{\mathcal{X}}\left(\mathcal{X}^{[\mathbf{m}]}\right) = 0.$$

Hence,  $(b - \beta) \mathcal{X}^{[\mathbf{m}]} \subseteq \text{Ker}(\pi^{\mathcal{X}})$ . Combining this with  $\text{Ker}(\pi^{\mathcal{X}}) \subseteq (b - \beta) \mathcal{X}^{[\mathbf{m}]}$ , we obtain  $\text{Ker}(\pi^{\mathcal{X}}) = (b - \beta) \mathcal{X}^{[\mathbf{m}]}$ . This proves Lemma 2.26 (d).

(e) The definition of the map  $D$  was canonical with respect to the base ring. Thus, the map  $D^{[\mathbf{m}]}$  (defined in the same way as  $D$ , but using the base ring  $\mathbf{m}$  instead of  $\mathbf{k}$ ) and the map  $D$  fit into a commutative diagram

$$\begin{array}{ccc} \mathcal{X}^{[\mathbf{m}]} & \xrightarrow{D^{[\mathbf{m}]}} & \mathcal{T}'^{[\mathbf{m}]} \\ \pi^{\mathcal{X}} \downarrow & & \downarrow \pi^{\mathcal{T}'} \\ \mathcal{X} & \xrightarrow{D} & \mathcal{T}' \end{array}$$

The commutativity of this diagram shows that  $\pi^{T'} \circ D^{[\mathbf{m}]} = D \circ \pi^{\mathcal{X}}$ . This proves Lemma 2.26 (e).  $\square$

**Lemma 2.27.** Let  $\beta \in \mathbf{k}$  be arbitrary. Let  $p \in \mathcal{X}$  be a pathless polynomial such that  $p \in \mathcal{J}_\beta$ . Then,  $D(p) = 0$ .

*Proof of Lemma 2.27.* Lemma 2.26 (c) (applied to  $f = p$ ) shows that there exists a pathless polynomial  $g \in \mathcal{X}^{[\mathbf{m}]}$  satisfying  $p = \pi^{\mathcal{X}}(g)$ . Fix such a  $g$ , and denote it by  $v$ . Thus,  $v \in \mathcal{X}^{[\mathbf{m}]}$  is a pathless polynomial satisfying  $p = \pi^{\mathcal{X}}(v)$ .

Lemma 2.26 (b) shows that  $\mathcal{J}_\beta = \pi^{\mathcal{X}}(\mathcal{J}_b^{[\mathbf{m}]})$ . Now,  $p \in \mathcal{J}_\beta = \pi^{\mathcal{X}}(\mathcal{J}_b^{[\mathbf{m}]})$ .

Hence, there exists some  $u \in \mathcal{J}_b^{[\mathbf{m}]}$  such that  $p = \pi^{\mathcal{X}}(u)$ . Consider this  $u$ .

The map  $\pi^{\mathcal{X}}$  is a  $\mathbf{k}$ -algebra homomorphism. Thus,  $\pi^{\mathcal{X}}(u - v) = \underbrace{\pi^{\mathcal{X}}(u)}_{=p} - \underbrace{\pi^{\mathcal{X}}(v)}_{=p} =$

$p - p = 0$ . Hence,  $u - v \in \text{Ker}(\pi^{\mathcal{X}}) = (b - \beta) \mathcal{X}^{[\mathbf{m}]}$  (by Lemma 2.26 (d)). In other words, there exists some  $w \in \mathcal{X}^{[\mathbf{m}]}$  such that  $u - v = (b - \beta) w$ . Consider this  $w$ .

From  $u - v = (b - \beta) w$ , we obtain  $u = v + (b - \beta) w$ .

Proposition 1.5 (applied to  $\mathbf{m}$ ,  $b$ ,  $\mathcal{X}^{[\mathbf{m}]}$ ,  $\mathcal{J}_b^{[\mathbf{m}]}$  and  $w$  instead of  $\mathbf{k}$ ,  $\beta$ ,  $\mathcal{X}$ ,  $\mathcal{J}_\beta$  and  $p$ ) shows that there exists a pathless polynomial  $q \in \mathcal{X}^{[\mathbf{m}]}$  such that  $w \equiv q \bmod \mathcal{J}_b^{[\mathbf{m}]}$ . Consider this  $q$ . We have

$$v + (b - \beta) \underbrace{q}_{\equiv w \bmod \mathcal{J}_b^{[\mathbf{m}]}} \equiv v + (b - \beta) w = u \equiv 0 \bmod \mathcal{J}_b^{[\mathbf{m}]}$$

(since  $u \in \mathcal{J}_b^{[\mathbf{m}]}$ ). In other words,  $v + (b - \beta) q \in \mathcal{J}_b^{[\mathbf{m}]}$ .

The element  $b$  of  $\mathbf{m}$  is regular (by Lemma 2.26 (a)). The polynomial  $v + (b - \beta) q \in \mathcal{X}^{[\mathbf{m}]}$  is pathless (since it is an  $\mathbf{m}$ -linear combination of the two pathless polynomials  $v$  and  $q$ ) and satisfies  $v + (b - \beta) q \in \mathcal{J}_b^{[\mathbf{m}]}$  (as we have shown). Hence, Lemma 2.23 (applied to  $\mathbf{m}$ ,  $b$ ,  $\mathcal{X}^{[\mathbf{m}]}$ ,  $\mathcal{J}_b^{[\mathbf{m}]}$ ,  $\mathcal{T}'^{[\mathbf{m}]}$ ,  $D^{[\mathbf{m}]}$  and  $v + (b - \beta) q$  instead of  $\mathbf{k}$ ,  $\beta$ ,  $\mathcal{X}$ ,  $\mathcal{J}_\beta$ ,  $\mathcal{T}'$ ,  $D$  and  $p$ ) shows that  $D^{[\mathbf{m}]}(v + (b - \beta) q) = 0$ .

But Lemma 2.26 (e) yields  $\pi^{T'} \circ D^{[\mathbf{m}]} = D \circ \pi^{\mathcal{X}}$ . Hence,

$$\begin{aligned} \underbrace{(D \circ \pi^{\mathcal{X}})}_{=\pi^{T'} \circ D^{[\mathbf{m}]}}(v + (b - \beta) q) &= (\pi^{T'} \circ D^{[\mathbf{m}]}) (v + (b - \beta) q) \\ &= \pi^{T'} \left( \underbrace{D^{[\mathbf{m}]}(v + (b - \beta) q)}_{=0} \right) = \pi^{T'}(0) = 0. \end{aligned}$$

Thus,

$$\begin{aligned}
 0 &= (D \circ \pi^{\mathcal{X}}) (v + (b - \beta) q) = D \left( \underbrace{\pi^{\mathcal{X}} (v + (b - \beta) q)}_{\substack{= \pi^{\mathcal{X}}(v) + \pi^{\mathcal{X}}((b - \beta)q) \\ \text{(since } \pi^{\mathcal{X}} \text{ is a } \mathbf{k}\text{-algebra homomorphism)}}} \right) \\
 &= D \left( \pi^{\mathcal{X}} (v) + \pi^{\mathcal{X}} ((b - \beta) q) \right). \tag{9}
 \end{aligned}$$

But  $(b - \beta) \underbrace{q}_{\in \mathcal{X}^{[\mathbf{m}]}} \in (b - \beta) \mathcal{X}^{[\mathbf{m}]} = \text{Ker}(\pi^{\mathcal{X}})$  and thus  $\pi^{\mathcal{X}}((b - \beta) q) = 0$ .

Thus, (9) becomes

$$0 = D \left( \pi^{\mathcal{X}} (v) + \underbrace{\pi^{\mathcal{X}} ((b - \beta) q)}_{=0} \right) = D \left( \underbrace{\pi^{\mathcal{X}} (v)}_{=p} \right) = D(p).$$

This proves Lemma 2.27.  $\square$

*Proof of Theorem 1.7.* Theorem 1.7 follows from Lemma 2.27 in the same way as we derived Lemma 2.21 from Lemma 2.20 (with the only difference that  $\mathcal{J}_1$  is replaced by  $\mathcal{J}_\beta$  throughout the proof).  $\square$

### 2.13. Appendix: Detailed proof of Proposition 1.5

Let us now pay a debt and explain the proof of Proposition 1.5 in full detail.

We begin with a few definitions:

**Definition 2.28.** Let  $\mathcal{X}_{\text{pathless}}$  denote the  $\mathbf{k}$ -submodule of  $\mathcal{X}$  spanned by all pathless monomials  $\mathbf{m} \in \mathfrak{M}$ . Thus,  $\mathcal{X}_{\text{pathless}}$  is the set of all pathless polynomials  $f \in \mathcal{X}$ .

**Definition 2.29.** Let  $\mathbf{m} \in \mathfrak{M}$  be a monomial. The *weight* of  $\mathbf{m}$  is defined to be  $\sum_{\substack{(i,j) \in [n]^2; \\ i < j}} a_{i,j} (n - j + i)$ , where the monomial  $\mathbf{m}$  has been written in the form  $\mathbf{m} = \prod_{\substack{(i,j) \in [n]^2; \\ i < j}} x_{i,j}^{a_{i,j}}$  (with  $a_{i,j} \in \mathbb{N}$ ). This weight is an integer, and will be denoted by  $\text{weight } \mathbf{m}$ .

Observe the following properties of weights:

**Lemma 2.30. (a)** For any  $(i, j) \in [n]^2$  satisfying  $i < j$ , we have  $\text{weight}(x_{i,j}) = n - j + i$ .

**(b)** If  $p \in \mathfrak{M}$  and  $q \in \mathfrak{M}$  are two monomials, then  $\text{weight}(pq) = \text{weight } p + \text{weight } q$ .

**(c)** If  $m \in \mathfrak{M}$  is a monomial, then  $\text{weight } m \in \mathbb{N}$ .

*Proof of Lemma 2.30.* Parts **(a)** and **(b)** of Lemma 2.30 are left to the reader.

Let us observe that every  $(i, j) \in [n]^2$  satisfies

$$n - \underbrace{j}_{\substack{\leq n \\ \text{(since } j \in [n])}} + \underbrace{i}_{\substack{> 0 \\ \text{(since } i \in [n])}} \geq n - n + 0 = 0. \quad (10)$$

**(c)** Let  $m \in \mathfrak{M}$  be a monomial. Write the monomial  $m$  in the form  $m = \prod_{\substack{(i,j) \in [n]^2; \\ i < j}} x_{i,j}^{a_{i,j}}$  (with  $a_{i,j} \in \mathbb{N}$ ). Then, the definition of  $\text{weight } m$  yields

$$\text{weight } m = \sum_{\substack{(i,j) \in [n]^2; \\ i < j}} \underbrace{a_{i,j}}_{\geq 0} \underbrace{(n - j + i)}_{\substack{\geq 0 \\ \text{(by (10))}}} \geq \sum_{\substack{(i,j) \in [n]^2; \\ i < j}} 0 \cdot 0 = 0.$$

Hence,  $\text{weight } m \in \mathbb{N}$ . This proves Lemma 2.30 **(c)**.  $\square$

**Lemma 2.31.** Let  $m \in \mathfrak{M}$  be a monomial. Then,  $m \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ .

*Proof of Lemma 2.31.* We shall prove Lemma 2.31 by strong induction over  $\text{weight } m$ .

<sup>16</sup> Thus, we fix any  $N \in \mathbb{N}$ , and we assume (as the induction hypothesis) that Lemma 2.31 holds in the case when  $\text{weight } m < N$ . We then must show that Lemma 2.31 holds in the case when  $\text{weight } m = N$ .

We have assumed that Lemma 2.31 holds in the case when  $\text{weight } m < N$ . In other words,

$$\left( \begin{array}{l} \text{if } m \in \mathfrak{M} \text{ is a monomial such that } \text{weight } m < N, \\ \text{then } m \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta \end{array} \right). \quad (11)$$

Now, fix a monomial  $m \in \mathfrak{M}$  such that  $\text{weight } m = N$ . We shall show that  $m \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ .

If  $m$  is pathless, then this is obvious<sup>17</sup>. Hence, for the rest of this proof, we WLOG assume that  $m$  is not pathless. In other words, there exists a triple

<sup>16</sup>This is legitimate, since Lemma 2.30 **(c)** shows that  $\text{weight } m \in \mathbb{N}$  in the situation of Lemma 2.31.

<sup>17</sup>*Proof.* Assume that  $m$  is pathless. We must then show that  $m \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ .

But recall that the  $\mathbf{k}$ -module  $\mathcal{X}_{\text{pathless}}$  is spanned by the pathless monomials. Thus,  $m \in \mathcal{X}_{\text{pathless}}$  (since  $m$  is a pathless monomial). Hence,  $m \in \mathcal{X}_{\text{pathless}} \subseteq \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ , qed.

$(i, j, k) \in [n]^3$  satisfying  $i < j < k$  and  $x_{i,j}x_{j,k} \mid \mathfrak{m}$  (as monomials). Consider such a triple  $(i, j, k)$ .

We have  $x_{i,j}x_{j,k} \mid \mathfrak{m}$  (as monomials). In other words, there exists a monomial  $\mathfrak{n} \in \mathfrak{M}$  such that  $\mathfrak{m} = x_{i,j}x_{j,k}\mathfrak{n}$ . Consider this  $\mathfrak{n}$ .

We have  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta) \in \mathcal{J}_\beta$  (since  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta)$  is one of the designated generators of the ideal  $\mathcal{J}_\beta$ ). Thus,

$x_{i,j}x_{j,k} \equiv x_{i,k}(x_{i,j} + x_{j,k} + \beta) \pmod{\mathcal{J}_\beta}$ . Now,

$$\begin{aligned} \mathfrak{m} &= \underbrace{x_{i,j}x_{j,k}}_{\equiv x_{i,k}(x_{i,j} + x_{j,k} + \beta) \pmod{\mathcal{J}_\beta}} \mathfrak{n} \equiv x_{i,k}(x_{i,j} + x_{j,k} + \beta) \mathfrak{n} \\ &= x_{i,k}x_{i,j}\mathfrak{n} + x_{i,k}x_{j,k}\mathfrak{n} + \beta x_{i,k}\mathfrak{n} \pmod{\mathcal{J}_\beta}. \end{aligned}$$

In other words,

$$\mathfrak{m} \in x_{i,k}x_{i,j}\mathfrak{n} + x_{i,k}x_{j,k}\mathfrak{n} + \beta x_{i,k}\mathfrak{n} + \mathcal{J}_\beta. \quad (12)$$

We shall now analyze the three monomials  $x_{i,k}x_{i,j}\mathfrak{n}$ ,  $x_{i,k}x_{j,k}\mathfrak{n}$  and  $x_{i,k}\mathfrak{n}$  on the right hand side of (12):

- We have  $\text{weight}(x_{i,k}x_{i,j}\mathfrak{n}) < N$ <sup>18</sup>. Hence, (11) (applied to  $x_{i,k}x_{i,j}\mathfrak{n}$  instead of  $\mathfrak{m}$ ) shows that

$$x_{i,k}x_{i,j}\mathfrak{n} \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta.$$

---

<sup>18</sup>*Proof.* We have  $\mathfrak{m} = x_{i,j}x_{j,k}\mathfrak{n} = x_{j,k}x_{i,j}\mathfrak{n}$  and thus

$$\begin{aligned} \text{weight} \underbrace{\mathfrak{m}}_{=x_{j,k}x_{i,j}\mathfrak{n}} &= \text{weight}(x_{j,k}x_{i,j}\mathfrak{n}) = \underbrace{\text{weight}(x_{j,k})}_{=n-k+j} + \text{weight}(x_{i,j}\mathfrak{n}) \\ &\quad \text{(by Lemma 2.30 (a), applied to } j \text{ and } k \text{ instead of } i \text{ and } j\text{)} \\ &\quad \text{(by Lemma 2.30 (b), applied to } \mathfrak{p} = x_{j,k} \text{ and } \mathfrak{q} = x_{i,j}\mathfrak{n}\text{)} \\ &= n - k + j + \text{weight}(x_{i,j}\mathfrak{n}). \end{aligned}$$

But Lemma 2.30 (b) (applied to  $\mathfrak{p} = x_{i,k}$  and  $\mathfrak{q} = x_{i,j}\mathfrak{n}$ ) shows that

$$\begin{aligned} \text{weight}(x_{i,k}x_{i,j}\mathfrak{n}) &= \underbrace{\text{weight}(x_{i,k})}_{=n-k+i} + \text{weight}(x_{i,j}\mathfrak{n}) = n - k + \underbrace{i}_{< j} + \text{weight}(x_{i,j}\mathfrak{n}) \\ &\quad \text{(by Lemma 2.30 (a), applied to } k \text{ instead of } j\text{)} \\ &< n - k + j + \text{weight}(x_{i,j}\mathfrak{n}) = \text{weight } \mathfrak{m} = N, \end{aligned}$$

qed.

- We have  $\text{weight}(x_{i,k}x_{j,k}\mathbf{n}) < N$ <sup>19</sup>. Hence, (11) (applied to  $x_{i,k}x_{j,k}\mathbf{n}$  instead of  $\mathbf{m}$ ) shows that

$$x_{i,k}x_{j,k}\mathbf{n} \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta.$$

- We have  $\text{weight}(x_{i,k}\mathbf{n}) < N$ <sup>20</sup>. Hence, (11) (applied to  $x_{i,k}\mathbf{n}$  instead of  $\mathbf{m}$ )

<sup>19</sup>*Proof.* We have

$$\begin{aligned} \text{weight}(\underbrace{\mathbf{m}}_{=x_{i,j}x_{j,k}\mathbf{n}}) &= \text{weight}(x_{i,j}x_{j,k}\mathbf{n}) = \underbrace{\text{weight}(x_{i,j})}_{=n-j+i} + \text{weight}(x_{j,k}\mathbf{n}) \\ &\quad \text{(by Lemma 2.30 (a))} \\ &\quad \text{(by Lemma 2.30 (b), applied to } \mathbf{p} = x_{i,j} \text{ and } \mathbf{q} = x_{j,k}\mathbf{n}) \\ &= n - j + i + \text{weight}(x_{j,k}\mathbf{n}). \end{aligned}$$

But Lemma 2.30 (b) (applied to  $\mathbf{p} = x_{i,k}$  and  $\mathbf{q} = x_{j,k}\mathbf{n}$ ) shows that

$$\begin{aligned} \text{weight}(x_{i,k}x_{j,k}\mathbf{n}) &= \underbrace{\text{weight}(x_{i,k})}_{=n-k+i} + \text{weight}(x_{j,k}\mathbf{n}) = n - \underbrace{k}_{>j} + i + \text{weight}(x_{j,k}\mathbf{n}) \\ &\quad \text{(by Lemma 2.30 (a), applied to } k \text{ instead of } j) \quad \text{(since } j < k) \\ &< n - j + i + \text{weight}(x_{j,k}\mathbf{n}) = \text{weight } \mathbf{m} = N, \end{aligned}$$

qed.

<sup>20</sup>*Proof.* We have

$$\begin{aligned} \text{weight}(\underbrace{\mathbf{m}}_{=x_{i,j}x_{j,k}\mathbf{n}}) &= \text{weight}(x_{i,j}x_{j,k}\mathbf{n}) = \underbrace{\text{weight}(x_{i,j})}_{=n-j+i} + \underbrace{\text{weight}(x_{j,k}\mathbf{n})}_{=\text{weight}(x_{j,k}) + \text{weight } \mathbf{n}} \\ &\quad \text{(by Lemma 2.30 (a))} \quad \text{(by Lemma 2.30 (b), applied to } \mathbf{p} = x_{j,k} \text{ and } \mathbf{q} = \mathbf{n}) \\ &\quad \text{(by Lemma 2.30 (b), applied to } \mathbf{p} = x_{i,j} \text{ and } \mathbf{q} = x_{j,k}\mathbf{n}) \\ &= n - j + i + \underbrace{\text{weight}(x_{j,k})}_{=n-k+j} + \text{weight } \mathbf{n} \\ &\quad \text{(by Lemma 2.30 (a), applied to } j \text{ and } k \text{ instead of } i \text{ and } j) \\ &= \underbrace{n - j + i + n - k + j}_{=n+n-k+i} + \text{weight } \mathbf{n} = \underbrace{n}_{>0} + n - k + i + \text{weight } \mathbf{n} \\ &> n - k + i + \text{weight } \mathbf{n}. \end{aligned}$$

But Lemma 2.30 (b) (applied to  $\mathbf{p} = x_{i,k}$  and  $\mathbf{q} = \mathbf{n}$ ) yields

$$\begin{aligned} \text{weight}(x_{i,k}\mathbf{n}) &= \underbrace{\text{weight}(x_{i,k})}_{=n-k+i} + \text{weight } \mathbf{n} = n - k + i + \text{weight } \mathbf{n} \\ &\quad \text{(by Lemma 2.30 (a), applied to } k \text{ instead of } j) \\ &< \text{weight } \mathbf{m} \quad \text{(since } \text{weight } \mathbf{m} > n - k + i + \text{weight } \mathbf{n}) \\ &= N, \end{aligned}$$

qed.



shows that

$$x_{i,k}\mathbf{n} \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta.$$

Now, (12) becomes

$$\begin{aligned} \mathbf{m} &\in \underbrace{x_{i,k}x_{i,j}\mathbf{n}}_{\in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta} + \underbrace{x_{i,k}x_{j,k}\mathbf{n}}_{\in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta} + \beta \underbrace{x_{i,k}\mathbf{n}}_{\in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta} + \underbrace{\mathcal{J}_\beta}_{\subseteq \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta} \\ &\subseteq (\mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta) + (\mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta) + \beta (\mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta) + (\mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta) \\ &\subseteq \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta \end{aligned}$$

(since  $\mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$  is a  $\mathbf{k}$ -module).

Now, let us forget that we fixed  $\mathbf{m}$ . We thus have shown that if  $\mathbf{m} \in \mathfrak{M}$  is a monomial such that  $\text{weight } \mathbf{m} = N$ , then  $\mathbf{m} \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ . In other words, Lemma 2.31 holds in the case when  $\text{weight } \mathbf{m} = N$ . This completes the induction step. Thus, Lemma 2.31 is proven.  $\square$

Now, we can prove Proposition 1.5:

*Proof of Proposition 1.5.* Lemma 2.31 shows that  $\mathbf{m} \in \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$  for each  $\mathbf{m} \in \mathfrak{M}$ . In other words,  $\mathfrak{M} \subseteq \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$  (where we consider  $\mathfrak{M}$  as being embedded into the polynomial ring  $\mathcal{X}$ ).

For any subset  $\mathcal{W}$  of  $\mathcal{X}$ , we let  $\text{span } \mathcal{W}$  denote the  $\mathbf{k}$ -submodule of  $\mathcal{X}$  spanned by  $\mathcal{W}$ . The set  $\mathfrak{M}$  spans the  $\mathbf{k}$ -module  $\mathcal{X}$  (since each polynomial  $f \in \mathcal{X}$  is a  $\mathbf{k}$ -linear combination of monomials  $\mathbf{m} \in \mathfrak{M}$ ). In other words,  $\mathcal{X} = \text{span } \mathfrak{M}$ . But from  $\mathfrak{M} \subseteq \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ , we obtain  $\text{span } \mathfrak{M} \subseteq \text{span } (\mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta) = \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$  (since  $\mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$  is a  $\mathbf{k}$ -submodule of  $\mathcal{X}$ ). Hence,  $\mathcal{X} = \text{span } \mathfrak{M} \subseteq \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ .

Now,  $p \in \mathcal{X} \subseteq \mathcal{X}_{\text{pathless}} + \mathcal{J}_\beta$ . In other words, there exist  $u \in \mathcal{X}_{\text{pathless}}$  and  $v \in \mathcal{J}_\beta$  such that  $p = u + v$ . Consider these  $u$  and  $v$ .

We have  $p = u + \underbrace{v}_{\in \mathcal{J}_\beta} \in u + \mathcal{J}_\beta$ . In other words,  $p \equiv u \pmod{\mathcal{J}_\beta}$ . But  $\mathcal{X}_{\text{pathless}}$

is the set of all pathless polynomials in  $\mathcal{X}$ . Thus,  $u$  is a pathless polynomial (since  $u \in \mathcal{X}_{\text{pathless}}$ ). Hence, there exists a pathless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_\beta}$  (namely,  $q = u$ ). This proves Proposition 1.5.  $\square$

### 3. Forkless polynomials and a basis of $\mathcal{X}/\mathcal{J}_\beta$

#### 3.1. Statements

We have thus answered one of the major questions about the ideal  $\mathcal{J}_\beta$ ; but we have begged perhaps the most obvious one: Can we find a basis of the  $\mathbf{k}$ -module  $\mathcal{X}/\mathcal{J}_\beta$ ? This turns out to be much simpler than the above; the key is to use a different strategy. Instead of reducing polynomials to pathless polynomials, we shall reduce them to *forkless* polynomials, defined as follows:

**Definition 3.1.** A monomial  $m \in \mathfrak{M}$  is said to be *forkless* if there exists no triple  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$  and  $x_{i,j}x_{j,k} \mid m$  (as monomials).

A polynomial  $p \in \mathcal{X}$  is said to be *forkless* if it is a  $\mathbf{k}$ -linear combination of forkless monomials.

The following characterization of forkless polynomials is rather obvious:

**Proposition 3.2.** Let  $m \in \mathfrak{M}$ . Then, the monomial  $m$  is forkless if and only if there exist a map  $f : [n-1] \rightarrow [n]$  and a map  $g : [n-1] \rightarrow \mathbb{N}$  such that

$$(f(i) > i \text{ for each } i \in [n-1]) \quad \text{and} \quad m = \prod_{i \in [n-1]} x_{i,f(i)}^{g(i)}.$$

Now, we claim the following:

**Theorem 3.3.** Let  $\beta \in \mathbf{k}$  and  $p \in \mathcal{X}$ . Then, there exists a **unique** forkless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_\beta}$ .

**Proposition 3.4.** Let  $\beta \in \mathbf{k}$  and  $p \in \mathcal{X}$ . The projections of the forkless monomials  $m \in \mathfrak{M}$  onto the quotient ring  $\mathcal{X}/\mathcal{J}_\beta$  form a basis of the  $\mathbf{k}$ -module  $\mathcal{X}/\mathcal{J}_\beta$ .

### 3.2. A reminder on Gröbner bases

Theorem 3.3 and Proposition 3.4 can be proven using the theory of Gröbner bases. See, e.g., [BecWei98] for an introduction. Let us outline the argument. We shall use the following concepts:

**Definition 3.5.** Let  $\Xi$  be a set of indeterminates. Let  $\mathcal{X}_\Xi$  be the polynomial ring  $\mathbf{k}[\xi \mid \xi \in \Xi]$  over  $\mathbf{k}$  in these indeterminates. Let  $\mathfrak{M}_\Xi$  be the set of all monomials in these indeterminates (i.e., the free abelian monoid on the set  $\Xi$ ). (For example, if  $\Xi = \{x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j\}$ , then  $\mathcal{X}_\Xi = \mathcal{X}$  and  $\mathfrak{M}_\Xi = \mathfrak{M}$ .)

(a) A *term order* on  $\mathfrak{M}_\Xi$  is a total order on the set  $\mathfrak{M}_\Xi$  that satisfies the following conditions:

- Each  $m \in \mathfrak{M}_\Xi$  satisfies  $1 \leq m$  (where 1 is the trivial monomial in  $\mathfrak{M}_\Xi$ ).
- If  $m, u$  and  $v$  are three elements of  $\mathfrak{M}_\Xi$  satisfying  $u \leq v$ , then  $mu \leq mv$ .

(b) If we are given a total order on the set  $\Xi$ , then we canonically obtain a term order on  $\mathfrak{M}_\Xi$  defined as follows: For two monomials  $m = \prod_{\xi \in \Xi} \xi^{m_\xi}$  and  $n = \prod_{\xi \in \Xi} \xi^{n_\xi}$  in  $\mathfrak{M}_\Xi$ , we set  $m \leq n$  if and only if either  $m = n$  or the largest

$\xi \in \Xi$  for which  $m_\xi$  and  $n_\xi$  differ satisfies  $m_\xi < n_\xi$ . This term order is called the *inverse lexicographical order* on the set  $\mathfrak{M}_\Xi$  determined by the given total order on  $\Xi$ .

(c) Two monomials  $m = \prod_{\xi \in \Xi} \xi^{m_\xi}$  and  $n = \prod_{\xi \in \Xi} \xi^{n_\xi}$  in  $\mathfrak{M}_\Xi$  are said to be *non-disjoint* if there exists some  $\xi \in \Xi$  satisfying  $m_\xi > 0$  and  $n_\xi > 0$ . Otherwise,  $m$  and  $n$  are said to be *disjoint*.

From now on, let us assume that some term order on  $\mathfrak{M}_\Xi$  has been chosen. The next definitions will all rely on this term order.

(d) If  $f \in \mathcal{X}_\Xi$  is a nonzero polynomial, then the *head term* of  $f$  denotes the largest  $m \in \mathfrak{M}_\Xi$  such that the coefficient of  $m$  in  $f$  is nonzero. This head term will be denoted by  $\text{HT}(f)$ . Furthermore, if  $f \in \mathcal{X}_\Xi$  is a nonzero polynomial, then the *head coefficient* of  $f$  is defined to be the coefficient of  $\text{HT}(f)$  in  $f$ ; this coefficient will be denoted by  $\text{HC}(f)$ .

(e) A nonzero polynomial  $f \in \mathcal{X}_\Xi$  is said to be *monic* if its head coefficient  $\text{HC}(f)$  is 1.

(f) If  $m = \prod_{\xi \in \Xi} \xi^{m_\xi}$  and  $n = \prod_{\xi \in \Xi} \xi^{n_\xi}$  are two monomials in  $\mathfrak{M}_\Xi$ , then the *lowest common multiple*  $\text{lcm}(m, n)$  of  $m$  and  $n$  is defined to be the monomial  $\prod_{\xi \in \Xi} \xi^{\max\{m_\xi, n_\xi\}}$ . (Thus,  $\text{lcm}(m, n) = mn$  if and only if  $m$  and  $n$  are disjoint.)

(g) If  $g_1$  and  $g_2$  are two monic polynomials in  $\mathcal{X}_\Xi$ , then the *S-polynomial* of  $g_1$  and  $g_2$  is defined to be the polynomial  $s_1 g_1 - s_2 g_2$ , where  $s_1$  and  $s_2$  are the unique two monomials satisfying  $s_1 \text{HT}(g_1) = s_2 \text{HT}(g_2) = \text{lcm}(\text{HT}(g_1), \text{HT}(g_2))$ . This S-polynomial is denoted by  $\text{spol}(g_1, g_2)$ .

From now on, let  $G$  be a subset of  $\mathcal{X}_\Xi$  that consists of monic polynomials.

(h) We define a binary relation  $\xrightarrow[G]{}$  on the set  $\mathcal{X}_\Xi$  as follows: For two polynomials  $f$  and  $g$  in  $\mathcal{X}_\Xi$ , we set  $f \xrightarrow[G]{} g$  (and say that  $f$  *reduces to  $g$  modulo  $G$* ) if there exists some  $p \in G$  and some monomials  $t \in \mathfrak{M}_\Xi$  and  $s \in \mathfrak{M}_\Xi$  with the following properties:

- The coefficient of  $t$  in  $f$  is  $\neq 0$ .
- We have  $s \cdot \text{HT}(p) = t$ .
- If  $a$  is the coefficient of  $t$  in  $f$ , then  $g = f - a \cdot s \cdot p$ .

(i) We let  $\xrightarrow[G]{*}$  denote the reflexive-and-transitive closure of the relation  $\xrightarrow[G]{}.$

(j) We say that a monomial  $m \in \mathfrak{M}_\Xi$  is *G-reduced* if it is not divisible by the head term of any element of  $G$ .

(k) Let  $\mathcal{I}$  be an ideal of  $\mathcal{X}_\Xi$ . The set  $G$  is said to be a *Gröbner basis* of the ideal  $\mathcal{I}$  if and only if the set  $G$  generates  $\mathcal{I}$  and has the following two equivalent properties:

- For each  $p \in \mathcal{X}_\Xi$ , there is a unique  $G$ -reduced  $q \in \mathcal{X}_\Xi$  such that  $p \xrightarrow[G]{*} q$ .

- For each  $p \in \mathcal{I}$ , we have  $p \xrightarrow[G]{*} 0$ .

The definition we just gave is modelled after the definitions in [BecWei98, Chapter 5]; however, there are several minor differences:

- We use the word “monomial” in the same meaning as [BecWei98, Chapter 5] use the word “term” (but not in the same meaning as [BecWei98, Chapter 5] use the word “monomial”).
- We allow  $\mathbf{k}$  to be a commutative ring, whereas [BecWei98, Chapter 5] require  $\mathbf{k}$  to be a field. This leads to some complications in the theory of Gröbner bases; in particular, not every ideal has a Gröbner basis anymore. However, everything **we** are going to use about Gröbner bases in this paper is still true in our general setting.
- We require the elements of the Gröbner basis  $G$  to be monic, whereas [BecWei98, Chapter 5] merely assume them to be nonzero polynomials. In this way, we are sacrificing some of the generality of [BecWei98, Chapter 5] (a sacrifice necessary to ensure that things don’t go wrong when  $\mathbf{k}$  is not a field). However, this is not a major loss of generality, since in the situation of [BecWei98, Chapter 5] the difference between monic polynomials and arbitrary nonzero polynomials is not particularly large (we can scale any nonzero polynomial by a constant scalar to obtain a monic polynomial, and so we can assume the polynomials to be monic in most of the proofs).

The following criterion for a set to be a Gröbner basis is well-known (it is, in fact, the main ingredient in the proof of the correctness of Buchberger’s algorithm):

**Proposition 3.6.** Let  $\Xi$ ,  $\mathcal{X}_\Xi$  and  $\mathfrak{M}_\Xi$  be as in Definition 3.5. Let  $\mathcal{I}$  be an ideal of  $\mathcal{X}_\Xi$ . Let  $G$  be a subset of  $\mathcal{X}_\Xi$  that consists of monic polynomials. Assume that the set  $G$  generates  $\mathcal{I}$ . Then,  $G$  is a Gröbner basis of  $\mathcal{I}$  if and only if it has the following property:

- If  $g_1$  and  $g_2$  are any two elements of the set  $G$ , then  $\text{spol}(g_1, g_2) \xrightarrow[G]{*} 0$ .

Proofs of Proposition 3.6 (at least in the case when  $\mathbf{k}$  is a field) can be found in [BecWei98, Theorem 5.48, (iii)  $\iff$  (i)], [EneHer12, Theorem 2.14], [Graaf16, Theorem 1.1.33], [MalBlo15, V.3 i)  $\iff$  ii)], [Monass02, Théorème (Buchberger)]

(i)  $\iff$  (ii)], and (in a slight variation) in [CoLiOs15, Chapter 2, §6, Theorem 6]<sup>21</sup>.

The following fact (known as “Buchberger’s first criterion”) somewhat simplifies dealing with S-polynomials:

**Proposition 3.7.** Let  $\Xi$ ,  $\mathcal{X}_\Xi$  and  $\mathfrak{M}_\Xi$  be as in Definition 3.5. Let  $G$  be a subset of  $\mathcal{X}_\Xi$  that consists of monic polynomials. Let  $g_1$  and  $g_2$  be two elements of the set  $G$  such that the head terms of  $g_1$  and  $g_2$  are disjoint. Then,  $\text{spol}(g_1, g_2) \xrightarrow[G]{*} 0$ .

Proposition 3.7 can be found in [BecWei98, Lemma 5.66], [Graaf16, Lemma 1.1.38], [EneHer12, Proposition 2.15], [MalBlo15, V.6 i)] and [Monass02, Lemme (in the section “Améliorations de l’algorithme”)]<sup>22</sup>.

We can combine Proposition 3.6 with Proposition 3.7 to obtain the following fact:

**Proposition 3.8.** Let  $\Xi$ ,  $\mathcal{X}_\Xi$  and  $\mathfrak{M}_\Xi$  be as in Definition 3.5. Let  $\mathcal{I}$  be an ideal of  $\mathcal{X}_\Xi$ . Let  $G$  be a subset of  $\mathcal{X}_\Xi$  that consists of monic polynomials. Assume that the set  $G$  generates  $\mathcal{I}$ . Then,  $G$  is a Gröbner basis of  $\mathcal{I}$  if and only if it has the following property:

- If  $g_1$  and  $g_2$  are two elements of the set  $G$  such that the head terms of  $g_1$  and  $g_2$  are non-disjoint, then  $\text{spol}(g_1, g_2) \xrightarrow[G]{*} 0$ .

Proposition 3.8 follows trivially from Proposition 3.6 after recalling Proposition 3.7. Explicitly, Proposition 3.8 appears (at least in the case when  $\mathbf{k}$  is a field) in [BecWei98, Theorem 5.68, (iii)  $\iff$  (i)] and [Graaf16, Conclusion after the proof of Lemma 1.1.38].

We shall also use the following simple fact:

**Proposition 3.9.** Let  $\Xi$ ,  $\mathcal{X}_\Xi$  and  $\mathfrak{M}_\Xi$  be as in Definition 3.5. Let  $\mathcal{I}$  be an ideal of  $\mathcal{X}_\Xi$ . Let  $G$  be a Gröbner basis of  $\mathcal{I}$ . The projections of the  $G$ -reduced monomials onto the quotient ring  $\mathcal{X}_\Xi/\mathcal{I}$  form a basis of the  $\mathbf{k}$ -module  $\mathcal{X}_\Xi/\mathcal{I}$ .

Proposition 3.9 is easy to prove; it also appears (in the case when  $\mathbf{k}$  is a field) in various texts (e.g., [CoLiOs15, Chapter 5, §3, Proposition 1 and Proposition 4], [Monass02, Théorème in the section “Espaces quotients”] or [Sturm08, Theorem 1.2.6]).

<sup>21</sup>Different sources state slightly different versions of Proposition 3.6. For example, some texts require  $\text{spol}(g_1, g_2) \xrightarrow[G]{*} 0$  not for any two elements  $g_1$  and  $g_2$  of  $G$ , but only for any two **distinct** elements  $g_1$  and  $g_2$  of  $G$ . However, this makes no difference, because if  $g_1$  and  $g_2$  are equal, then  $\text{spol}(g_1, g_2) = 0 \xrightarrow[G]{*} 0$ . Similarly, other texts require  $g_1 < g_2$  (with respect to some chosen total order on  $G$ ); this also does not change much, since  $\text{spol}(g_1, g_2) = -\text{spol}(g_2, g_1)$ .

<sup>22</sup>That said, the proof of [Monass02, Lemme (in the section “Améliorations de l’algorithme”)] is incorrect.

### 3.3. The proofs

The main workhorse of the proofs is the following fact:

**Proposition 3.10.** Let  $\beta \in \mathbf{k}$  and  $p \in \mathcal{X}$ . Consider the inverse lexicographical order on the set  $\mathfrak{M}$  of monomials determined by

$$\begin{aligned} x_{1,2} &> x_{1,3} > \cdots > x_{1,n} \\ &> x_{2,3} > x_{2,4} > \cdots > x_{2,n} \\ &> \cdots \\ &> x_{n-1,n}. \end{aligned}$$

Then, the set

$$\left\{ x_{i,k}x_{i,j} - x_{i,j}x_{j,k} + x_{i,k}x_{j,k} + \beta x_{i,k} \mid (i,j,k) \in [n]^3 \text{ satisfying } i < j < k \right\} \quad (13)$$

is a Gröbner basis of the ideal  $\mathcal{J}_\beta$  of  $\mathcal{X}$  (with respect to this order).

*Proof of Proposition 3.10 (sketched).* The elements  $x_{i,k}x_{i,j} - x_{i,j}x_{j,k} + x_{i,k}x_{j,k} + \beta x_{i,k}$  of the set (13) differ from the designated generators  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta)$  of the ideal  $\mathcal{J}_\beta$  merely by a factor of  $-1$  (indeed,  $x_{i,k}x_{i,j} - x_{i,j}x_{j,k} + x_{i,k}x_{j,k} + \beta x_{i,k} = (-1)(x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta))$ ). Thus, they generate the ideal  $\mathcal{J}_\beta$ . Hence, in order to prove that they form a Gröbner basis of  $\mathcal{J}_\beta$ , we merely need to show the following claim:

*Claim 1:* Let  $g_1$  and  $g_2$  be two elements of the set (13) such that the head terms of  $g_1$  and  $g_2$  are non-disjoint. Then,  $\text{spol}(g_1, g_2) \xrightarrow[G]{*} 0$ , where  $G$  is the set (13).

(Indeed, proving Claim 1 is sufficient because of Proposition 3.8.)

In order to prove Claim 1, we fix two elements  $g_1$  and  $g_2$  of the set (13) such that the head terms of  $g_1$  and  $g_2$  are non-disjoint. Thus,

$$g_1 = x_{i_1,k_1}x_{i_1,j_1} - x_{i_1,j_1}x_{j_1,k_1} + x_{i_1,k_1}x_{j_1,k_1} + \beta x_{i_1,k_1}$$

for some  $(i_1, j_1, k_1) \in [n]^3$  satisfying  $i_1 < j_1 < k_1$ , and

$$g_2 = x_{i_2,k_2}x_{i_2,j_2} - x_{i_2,j_2}x_{j_2,k_2} + x_{i_2,k_2}x_{j_2,k_2} + \beta x_{i_2,k_2}.$$

for some  $(i_2, j_2, k_2) \in [n]^3$  satisfying  $i_2 < j_2 < k_2$ . Since the head terms  $x_{i_1,k_1}x_{i_1,j_1}$  and  $x_{i_2,k_2}x_{i_2,j_2}$  of  $g_1$  and  $g_2$  are non-disjoint, we must have  $i_1 = i_2$ . Furthermore, one of  $j_1$  and  $k_1$  must equal one of  $j_2$  and  $k_2$  (for the same reason). Thus, there are at most four distinct integers among  $i_1, i_2, j_1, j_2, k_1, k_2$ .

We can now finish off Claim 1 by straightforward computations, after distinguishing several cases based upon which of the numbers  $j_1$  and  $k_1$  equal which

of the numbers  $j_2$  and  $k_2$ . We WLOG assume that  $(i_1, j_1, k_1) \neq (i_2, j_2, k_2)$  (since otherwise, it is clear that  $\text{spol}(g_1, g_2) = 0 \xrightarrow[G]{*} 0$ ). Thus, there are **exactly** four distinct integers among  $i_1, i_2, j_1, j_2, k_1, k_2$  (since  $i_1 = i_2$ , since  $i_1 < j_1 < k_1$  and  $i_2 < j_2 < k_2$ , and since one of  $j_1$  and  $k_1$  equals one of  $j_2$  and  $k_2$ ). Let us denote these four integers by  $a, b, c, d$  in increasing order<sup>23</sup> (so that  $a < b < c < d$ ). Hence,  $i_1 = a$  (since  $i_1 < j_1 < k_1$  and  $i_2 < j_2 < k_2$ ), whereas the two pairs  $(j_1, k_1)$  and  $(j_2, k_2)$  are two of the three pairs  $(b, c)$ ,  $(b, d)$  and  $(c, d)$  (for the same reason). Hence,  $g_1$  and  $g_2$  are two of the three polynomials

$$\begin{aligned} & x_{a,c}x_{a,b} - x_{a,b}x_{b,c} + x_{a,c}x_{b,c} + \beta x_{a,c}, \\ & x_{a,d}x_{a,b} - x_{a,b}x_{b,d} + x_{a,d}x_{b,d} + \beta x_{a,d}, \\ & x_{a,d}x_{a,c} - x_{a,c}x_{c,d} + x_{a,d}x_{c,d} + \beta x_{a,d}. \end{aligned}$$

What remains is the straightforward verification that  $\text{spol}(g_1, g_2) \xrightarrow[G]{*} 0$ ; this is easily done by hand.

Thus, Proposition 3.10 is proven.  $\square$

*Proof of Proposition 3.4 (sketched).* Let  $G_\beta$  be the set (13). Then, Proposition 3.10 shows that  $G_\beta$  is a Gröbner basis of the ideal  $\mathcal{J}_\beta$  of  $\mathcal{X}$  (where  $\mathfrak{M}$  is endowed with the term order defined in Proposition 3.10). Hence, Proposition 3.9 (applied to  $\Xi = \{x_{i,j} \mid (i,j) \in [n]^2 \text{ satisfying } i < j\}$ ,  $\mathcal{X}_\Xi = \mathcal{X}$ ,  $\mathfrak{M}_\Xi = \mathfrak{M}$ ,  $\mathcal{I} = \mathcal{J}_\beta$  and  $G = G_\beta$ ) shows that the projections of the  $G_\beta$ -reduced monomials onto the quotient ring  $\mathcal{X}/\mathcal{J}_\beta$  form a basis of the  $\mathbf{k}$ -module  $\mathcal{X}/\mathcal{J}_\beta$ . Since the  $G_\beta$ -reduced monomials are precisely the forkless monomials, this yields Proposition 3.4.  $\square$

*Proof of Theorem 3.3 (sketched).* Theorem 3.3 is merely a restatement of Proposition 3.4.  $\square$

Let us notice that the “existence” part of Theorem 3.3 can also be proven similarly to how we proved Proposition 1.5.<sup>24</sup> Is there a similarly simple argument for the “uniqueness” part?

## 4. A generalization?

The ideals  $\mathcal{J}_\beta$  of the  $\mathbf{k}$ -algebra  $\mathcal{X}$  can be “deformed” by introducing a second parameter  $\alpha \in \mathbf{k}$ , leading to the following definition:

<sup>23</sup>This integer  $b$  has nothing to do with the indeterminate  $b$  from Definition 2.25.

<sup>24</sup>This time, we need to define a different notion of “weight”: Instead of defining the weight of a monomial  $\mathfrak{m} = \prod_{\substack{(i,j) \in [n]^2; \\ i < j}} x_{i,j}^{a_{i,j}}$  to be  $\text{weight } \mathfrak{m} = \sum_{\substack{(i,j) \in [n]^2; \\ i < j}} a_{i,j}(n - j + i)$ , we now must define it to be  $\text{weight } \mathfrak{m} = \sum_{\substack{(i,j) \in [n]^2; \\ i < j}} a_{i,j}(j - i)$ .

**Definition 4.1.** Let  $\beta \in \mathbf{k}$  and  $\alpha \in \mathbf{k}$ . Let  $\mathcal{J}_{\beta,\alpha}$  be the ideal of  $\mathcal{X}$  generated by all elements of the form  $x_{i,j}x_{j,k} - x_{i,k}(x_{i,j} + x_{j,k} + \beta) - \alpha$  for  $(i, j, k) \in [n]^3$  satisfying  $i < j < k$ .

The idea of this definition again goes back to the work of Anatol Kirillov (see, e.g., [Kirill16, Definition 5.1 (1)] for a noncommutative variant of the quotient ring  $\mathcal{X}/\mathcal{J}_{\beta,\alpha}$ , which he calls the “associative quasi-classical Yang–Baxter algebra of weight  $(\alpha, \beta)$ ”). The ideal  $\mathcal{J}_\beta$  is a particular case:  $\mathcal{J}_\beta = \mathcal{J}_{\beta,0}$ .

Similarly to Proposition 1.5, we can prove the following:

**Proposition 4.2.** Let  $\beta \in \mathbf{k}$ ,  $\alpha \in \mathbf{k}$  and  $p \in \mathcal{X}$ . Then, there exists a pathless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_{\beta,\alpha}}$ .

It appears (based on computer experiments) that an analogue to Theorem 1.7 should also hold:

**Conjecture 4.3.** Let  $\beta \in \mathbf{k}$ ,  $\alpha \in \mathbf{k}$  and  $p \in \mathcal{X}$ . Consider any pathless polynomial  $q \in \mathcal{X}$  such that  $p \equiv q \pmod{\mathcal{J}_{\beta,\alpha}}$ . Then,  $D(q)$  does not depend on the choice of  $q$  (but merely on the choice of  $\beta$ ,  $\alpha$  and  $p$ ).

## References

- [BecWei98] Thomas Becker, Volker Weispfennig, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Corrected 2nd printing, Springer 1998.
- [CoLiOs15] David A. Cox, John Little, Donal O’Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, 4th edition, Springer 2015.
- [EneHer12] Viviana Ene, Jürgen Herzog, *Gröbner Bases in Commutative Algebra*, Graduate Studies in Mathematics #130, AMS 2012.
- [EscMes15] Laura Escobar, Karola Mészáros, *Subword complexes via triangulations of root polytopes*, arXiv:1502.03997v2.
- [Graaf16] Willem de Graaf, *Computational Algebra*, lecture notes, version 21 September 2016.  
<http://www.science.unitn.it/~degraaf/compalg/notes.pdf>
- [Kirill16] Anatol N. Kirillov, *On Some Quadratic Algebras I  $\frac{1}{2}$ : Combinatorics of Dunkl and Gaudin Elements, Schubert, Grothendieck, Fuss-Catalan, Universal Tutte and Reduced Polynomials*, SIGMA **12** (2016), 002, 172 pages, arXiv:1502.00426v3.



- [MalBlo15] Philippe Malbos, Thomas Blossier, *Algèbre appliquée: Introduction aux bases de Gröbner et à leurs applications*, lecture notes, version 4 May 2015.  
<http://math.univ-lyon1.fr/~malbos/Ens/algapip12.pdf>
- [Meszar09] Karola Mészáros, *Root polytopes, triangulations, and the subdivision algebra. I*, Trans. Amer. Math. Soc. 363 (2011), pp. 4359–4382.  
See also arXiv:0904.2194v3 for a preprint version.
- [Monass02] Denis Monasse, *Introduction aux bases de Gröbner: théorie et pratique*, lecture notes, version 19 November 2002.  
<http://denis.monasse.free.fr/denis/articles/grobner.pdf>
- [SageMath] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 7.6)*, 2017.
- [Stanle15] Richard P. Stanley, *Catalan Numbers*, Cambridge University Press 2015.
- [Sturmf08] Bernd Sturmfels, *Algorithms in Invariant Theory*, 2nd edition, Springer 2008.